FSA 2006/50

SENIOR MANAGEMENT ARRANGEMENTS, SYSTEMS AND CONTROLS (MARKETS IN FINANCIAL INSTRUMENTS AND CAPITAL REQUIREMENTS DIRECTIVES) INSTRUMENT 2006

Powers exercised

A. The Financial Services Authority makes this instrument in the exercise of the following powers and related provisions in the Financial Services and Markets Act 2000 ("the Act"):

(1) section 138 (General rule-making power);
(2) section 141 (Insurance business rules);
(3) section 145 (Financial promotion rules);
(4) section 146 (Money laundering rules);
(5) section 147 (Control of information rules);
(6) section 149 (Evidential provisions);
(7) section 150(2) (Actions for damages);
(8) section 156 (General supplementary powers); and
(9) section 157(1) (Guidance).

B. The rule-making powers listed above are specified for the purpose of section 153(2) (Rule-making instruments) of the Act.

Commencement

C. This instrument comes into force as follows:

(1) Annex C and E on 31 December 2006;
(2) Annex F, L and M on 1 November 2007;
(3) The remainder of this instrument comes into force on 1 January 2007.

Amendments to the Integrated Prudential Sourcebook and the Senior Management Arrangement, Systems and Controls Sourcebook

D. (1) In relation to the "Amended text" in column (3) of the table in D(5), SYSC is amended in accordance with Annex A of this instrument.

(2) In relation to the "New text" indicated in column (3), SYSC is amended by inserting the provisions in Annex B to this instrument.

(3) In relation to the "Transferred, Amended and New text" in column (3), SYSC is amended by inserting the provisions in Annex C in this instrument (which has the effect of transferring the provisions in PRU identified in column (2), with amendments, to the location indicated in column (1) and inserting new text in Annex C).

(4) In relation to the "Transferred and Amended text" in column (3), SYSC is amended by inserting the provisions in Annex D in this instrument (which has the effect of transferring the provisions in PRU identified in column (2), with amendments, to the location indicated in column (1)).

(4) In relation to the "Transferred text" in column (3), SYSC is amended by inserting the provisions of Annex E in this instrument (which has the effect of transferring the provisions in SYSC and PRU identified in column (2), with necessary consequential changes, to the location indicated in column (1)).

(5) The table referred to is:

(1) SYSC	(2) Current designation in PRU or SYSC (where applicable)	(3) Type of text	(4) Annex in this Instrument
SYSC TP		New text	Annex B
SYSC 1	SYSC 1	Amended text	Annex A
SYSC 3	SYSC 3	Amended text	Annex A
SYSC 4		New text	Annex B
SYSC 5		New text	Annex B
SYSC 6		New text	Annex B
SYSC 7		New text	Annex B
SYSC 8		New text	Annex B
SYSC 10		New text	Annex B
SYSC 11	PRU 5.1	Transferred and Amended and New text	Annex C
SYSC 12	PRU 8.1	Transferred and Amended text	Annex D
SYSC 13	SYSC 3A	Transferred text	Annex E
SYSC 14 (except 14.1.65G)	PRU 1.4	Transferred text	Annex E
SYSC 14.1.65G	PRU 6.1.9G	Transferred text	Annex E
SYSC 15	PRU 3.1	Transferred text	Annex E
SYSC 16	PRU 4.1	Transferred text	Annex E
SYSC 17	PRU 7.1	Transferred text	Annex E
SYSC 18	SYSC 4	Transferred text	Annex E
SYSC Schedule 1	SYSC Schedule 1	Amended text	Annex A
SYSC Schedule 5	SYSC Schedule 5	Amended text	Annex A
SYSC Schedule 6	SYSC Schedule 6	Amended text	Annex A

Further amendments to SYSC

E. SYSC is further amended by the provisions in Annex F to this instrument.

Amendments to the Glossary

F. The Glossary is amended by the provisions in Annex T to this instrument.

Amendments to the Handbook

G. The modules of the FSA's Handbook of rules and guidance listed in column (1) below are amended in accordance with the Annexes to this instrument listed in column (2).

(1)	(2)
Principles for Businesses sourcebook (PRIN)	Annex G
Threshold Conditions (COND)	Annex H
Conduct of Business sourcebook (COB)	Annex I
Insurance: Conduct of Business sourcebook (ICOB)	Annex J
Mortgages: Conduct of Business sourcebook (MCOB)	Annex K
Client Assets sourcebook (CASS)	Annex L
Market Conduct sourcebook (MAR)	Annex M
Training and Competence sourcebook (TC)	Annex N
Supervision manual (SUP)	Annex O
Enforcement manual (ENF)	Annex P
Credit Unions sourcebook (CRED)	Annex Q
Professional Firms sourcebook (PROF)	Annex R
Recognised Investment Exchanges and Recognised Clearing Houses sourcebook (REC)	Annex S

Citation

H. This instrument may be cited as the Senior Management Arrangements, Systems and Controls (Markets in Financial Instruments and Capital Requirements Directives) Instrument 2006.

By order of the Board
23 November 2006

Annex A

Senior Management Arrangements, Systems and Controls Handbook (SYSC)

In this Annex, underlining indicates new text and striking through indicates deleted text. Where an entire section of text is being inserted, the place where the change will be made is indicated and the text is not underlined.

1 Application and purpose

1.1 Application of SYSC 2 and SYSC 3

Purpose of this section

1.1.-2 G [deleted]

1.1.-1 G [deleted]

1.1.1 R Who?

SYSC 2 and *SYSC* 3 apply to every *firm* except that:

…

(c) *SYSC* 3 applies, but only with respect to the activities in *SYSC* 1.1.4 R; ~~and~~

(5) for an *authorised professional firm* when carrying on *non-mainstream regulated activities*, *SYSC* 3.2.6A R to *SYSC* 3.2.6J G do not apply~~.~~; and

(6) *SYSC* 3.2.23R to *SYSC* 3.2.36R apply only to a *BIPRU firm*.

…

1.2 Purpose of SYSC

1.2.1 G The purposes of *SYSC* are:

(1) to encourage *firms' directors* and *senior managers* to take appropriate practical responsibility for their *firms'* arrangements on matters likely to be of interest to the *FSA* because they impinge on the *FSA's* functions under the *Act*;

(2) to increase certainty by amplifying *Principle* 3, under which a *firm* must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems; ~~and~~

(3) to encourage *firms* to vest responsibility for effective and responsible organisation in specific *directors* and *senior managers*~~.~~;

(4) to create a common platform of organisational and systems and controls requirements for *firms* subject to the *CRD* and/or *MiFID*; and

(5) to set out high-level organisational and systems and controls requirements for *insurers*.

~~1.2.2 G The main matters, referred to in *SYSC*1.2.1G (1), which are likely to be of interest to the *FSA* are those which relate to confidence in the *financial system*; to the fair treatment of *firms' customers*; to the protection of *consumers*; and to the use of the *financial system* in connection with *financial crime*. The *FSA* is not primarily concerned with risks which threaten only the owners of a *financial business* except in so far as these risks may have an impact on those matters.~~

To be inserted after SYSC 1.2

1.3 Application of the common platform requirements

Who?

1.3.1 R The *common platform requirements* apply to a *common platform firm* unless provided otherwise in a specific *rule*.

1.3.1A G From 1 January 2007 until 1 November 2007, the application of the *common platform requirements* is limited by *SYSC* TP 1.

What?

1.3.2 R The *common platform organisational requirements* apply with respect to the carrying on of the following (unless provided otherwise within a specific *rule*):

(1) *regulated activities*;

(2) activities that constitute *dealing in investments as principal*, disregarding the exclusion in article 15 of the *Regulated Activities Order* (Absence of holding out etc); and

(3) *ancillary activities*.

1.3.3 G The application of the provisions on the conflicts of interest in *SYSC* 10 is set out in *SYSC* 10.1.1R and *SYSC* 10.2.1R.

1.3.4 R [To follow.]

1.3.5 R The *common platform requirements on financial crime* apply as set out in *SYSC* 1.3.2R, except that they do not apply:

(1) with respect to:

(a) activities that constitute *dealing in investments as principal*, disregarding the exclusion in article 15 of the *Regulated Activities Order* (Absence of holding out etc); and

(b) *ancillary activities*; or

(2) in relation to the following *regulated activities:*

(a) *general insurance business*;

(b) *insurance mediation activity* in relation to a *general insurance contract* or *pure protection contract*;

(c) *long-term insurance business* which is outside the *Consolidated Life Directive* (unless it is otherwise one of the *regulated activities* specified in this *rule*);

(d) business relating to contracts which are within the *Regulated Activities Order* only because they fall within paragraph (e) of the definition of "contract of insurance" in article 3 of that Order;

(e) (i) arranging by the *Society of Lloyd's* of deals in *general insurance contracts* written at Lloyd's; and

(ii) *managing the underwriting capacity of a Lloyd's syndicate as a managing agent at Lloyd's*; and

(f) *home finance mediation activity* and *administering a home finance transaction.*

1.3.6 R The *common platform organisational requirements*, except the *common platform requirements on financial crime*, also apply with respect to the *communication* and *approval* of *financial promotions* which:

(1) if *communicated* by an *unauthorised person* without *approval* would contravene section 21(1) of the *Act* (Restrictions on financial promotion); and

(2) may be *communicated* by a *firm* without contravening section 238(1) of the *Act* (Restrictions on promotion of collective investment schemes).

1.3.7 R The *common platform organisational requirements*, except the *common platform requirements on financial crime*, also:

(1) apply with respect to the carrying on of *unregulated activities* in a *prudential context*; and

(2) take into account any activity of other members of a *group* of which the *firm* is a member.

1.3.8 G *SYSC* 1.3.7R(2) does not mean that inadequacy of a *group* member's systems and controls will automatically lead to a *firm* contravening any of the *common platform organisational requirements*. Rather, the potential impact of a *group* member's activities, including its systems and controls, and any systems and controls that operate on a *group* basis, will be relevant in determining the appropriateness of the *firm's* own systems and controls.

Where?

1.3.9 R The *common platform requirements* apply to a *common platform firm* in relation to activities carried on by it from an establishment in the *United Kingdom*.

1.3.10 R The *common platform requirements*, except the *common platform requirements on financial crime*, apply to a *common platform firm* in relation to *passported activities* carried on by it from a *branch* in another *EEA State*.

1.3.11 R The *common platform organisational requirements*, except the *common platform requirements on financial crime*, also apply in a *prudential context* to a *UK domestic firm* with respect to activities wherever they are carried on.

Actions for damages

1.3.12 R A contravention of a *rule* in the *common platform requirements* does not give rise to a right of action by a *private person* under section 150 of the *Act* (and each of those *rules* is specified under section 150(2) of the *Act* as a provision giving rise to no such right of action).

1.4 Application of SYSC 11 to SYSC 18

What?

1.4.1 G The application of each of chapters *SYSC* 11 to *SYSC* 18 is set out in those chapters.

Actions for damages

1.4.2 R A contravention of a *rule* in *SYSC* 11 to *SYSC* 18 does not give rise to a right of action by a *private person* under section 150 of the *Act* (and each of those *rules* is specified under section 150(2) of the *Act* as a provision giving rise to no such right of action).

To be inserted after SYSC 3.1.1R

3.1.1A R *SYSC* 3.1 and *SYSC* 3.2.1G to *SYSC* 3.2.22G apply to a *BIPRU firm* only to the extent that they do not conflict with *SYSC* 3.2.23R to *SYSC* 3.2.36R.

…

To be inserted after SYSC 3.2.5G

Organisation

…

3.2.5A R An *overseas bank* must ensure that at least two individuals effectively direct its business.

3.2.5B G In the case of an *overseas bank*, the *FSA* assesses whether at least two individuals effectively direct the business of the *bank* (and not just the business of its branch in the *United Kingdom*). The *FSA* also takes into account the manner in which management decisions are taken in the *United Kingdom* branch in assessing the adequacy of the *overseas bank's* systems and controls.

…

To be inserted after SYSC 3.2.22G

CRD requirements

(1) General organisation requirements

3.2.23 R A *BIPRU firm* must have robust governance arrangements, which include a clear organisational structure with well defined, transparent and consistent lines of responsibility, effective processes to identify, manage, monitor and report the risks it is or might be exposed to, and adequate internal control mechanisms, including sound administrative and accounting procedures.

[Note: article 22(1) of the *Banking Consolidation Directive*]

3.2.24 R The arrangements, processes and mechanisms referred to in *SYSC* 3.2.23R must be comprehensive and proportionate to the nature, scale and complexity of the *BIPRU firm's* activities. The technical criteria laid down in *BIPRU* 2.3.7R(1), *BIPRU* 9.1.6R, *BIPRU* 9.13.21R (Liquidity plans), *BIPRU* 10.12.3R (Concentration risk policies), *SYSC* 3.2.26R and *SYSC* 3.2.28R to *SYSC* 3.2.36R must be taken into account.

[Note: article 22(2) of the *Banking Consolidation Directive*]

3.2.25 R A *BIPRU firm* must ensure that its internal control mechanisms and administrative and accounting procedures permit the verification of its compliance with *rules* adopted in accordance with the Capital Adequacy Directive at all times.

[Note: article 35(1) second sentence of the *Capital Adequacy Directive*]

3.2.26 R A *BIPRU firm* must have contingency and business continuity plans in place aimed at ensuring its ability to operate on an ongoing basis and limit losses in the event of severe business disruption.

[Note: annex V paragraph 13 of the *Banking Consolidation Directive*]

3.2.27 R A *credit institution* must have at least two persons who effectively direct the business of the *firm*. These persons must be of sufficiently good repute and have sufficient experience to perform their duties.

[Note: article 11(1) of the *Banking Consolidation Directive*]

(2) Employees, agents and other relevant persons

3.2.28 R The *governing body* of a *BIPRU firm* must define arrangements concerning the segregation of duties in the organisation and the prevention of conflicts of interest.

[Note: annex V paragraph 1 of the *Banking Consolidation Directive*]

(3) Risk control

3.2.29 R The *governing body* of a *BIPRU firm* must approve and periodically review the strategies and policies for taking up, managing, monitoring and mitigating the risks the *firm* is or might be exposed to, including those posed by the macroeconomic environment in which it operates in relation to the status of the business cycle.

[Note: annex V paragraph 2 of the *Banking Consolidation Directive*]

3.2.30 R A *BIPRU firm* must base credit-granting on sound and well-defined criteria and clearly establish the process for approving, amending, renewing, and re-financing credits.

[Note: annex V paragraph 3 of the *Banking Consolidation Directive*]

3.2.31 R A *BIPRU firm* must operate through effective systems the ongoing administration and monitoring of its various credit risk-bearing portfolios and exposures, including for identifying and managing problem credits and for making adequate value adjustments and provisions.

[Note: annex V paragraph 4 of the *Banking Consolidation Directive*]

3.2.32 R A *BIPRU firm* must adequately diversify credit portfolios given its target markets and overall credit strategy.

[Note: annex V paragraph 5 of the *Banking Consolidation Directive*]

3.2.33 R A *BIPRU firm* must address and control by means of written policies and procedures the risk that recognised credit risk mitigation techniques used by it prove less effective than expected.

[Note: annex V paragraph 6 of the *Banking Consolidation Directive*]

3.2.34 R A *BIPRU firm* must implement policies and processes for the measurement and management of all material sources and effects of market risks.

[Note: annex V paragraph 10 of the *Banking Consolidation Directive*]

3.2.35 R A *BIPRU firm* must implement systems to evaluate and manage the risk arising from potential changes in interest rates as they affect a *BIPRU firm's* non-trading activities.

[Note: annex V paragraph 11 of the *Banking Consolidation Directive*]

3.2.36 R A *BIPRU firm* must implement policies and processes to evaluate and manage the exposure to operational risk, including to low-frequency high severity events. Without prejudice to the definition of *operational risk*, *BIPRU firms* must articulate what constitutes operational risk for the purposes of those policies and procedures.

[Note: annex V paragraph 12 of the *Banking Consolidation Directive*]

Schedule 1 to be amended as follows:

…

Handbook reference	Subject of record	Contents of record	When record must be made	Retention period
…..				
SYSC 10.1.6R	Conflict of interest	Kinds of service or activity carried out by or on behalf of the *firm* in which a conflict of interest entailing a material risk of damage to the interests of one or more *clients* has arisen or, in the case of an ongoing service or activity, may arise.	Not specified	5 years
SYSC 14.1.53R	Prudential risk management and systems and controls	Accounting and other records that are sufficient to enable the *firm* to demonstrate to the *FSA*: (1) that the *firm* is financially sound and has appropriate systems and controls; (2) the *firm's* financial position and exposure to risk (to a reasonable degree of accuracy); (3) the *firm's* compliance with the *rules* in *GENPRU*, *INSPRU* and	Not specified	3 years, or longer as appropriate

		SYSC.		

Schedule 5 to be amended as follows

…

Chapter/ Appendix	**Section/ Annex**	**Paragraph**	**Right of action under section 150**		
			For private person?	**Removed?**	**For other person?**
~~All *rules* in~~ *SYSC* 2 and *SYSC* 3			No	Yes *SYSC* 1.1.12R	No
SYSC 4 to *SYSC* 10			No	Yes *SYSC* 1.3.12R	No
SYSC 11 to *SYSC* 18			No	Yes *SYSC* 1.4.2R	No

Schedule 6 to be amended as follows

Schedule 6	Rules that can be waived	
	G	The *rules* in *SYSC* can be *waived* by the *FSA* under section 148 of the *Act* (Modification or waiver of rules) in so far as this is compatible with the *United Kingdom's* responsibilities to implement the requirements of any European Directive .

Annex B

Senior Management Arrangements, Systems and Controls Handbook (SYSC)

In this Annex, all text in new and is not underlined.

To be inserted in SYSC Transchedule

TP Transitional provisions

TP 1 Common platform firms

Application

1.1 R *SYSC* TP 1 applies to a *common platform firm*.

Commencement and expiry of SYSC TP 1

1.2 R *SYSC* TP 1 comes into force on 1 January 2007 and applies until 1 November 2007.

Purpose

1.3 G From 1 November 2007, a *firm* must comply with the *common platform requirements* and *SYSC* 3 will cease to apply to it. However, until 1 November 2007, a *firm* may choose to comply with the specific parts of the *common platform requirements* instead of *SYSC* 3. The purpose of *SYSC* TP 1 is to give a *firm* the option of complying with the *common platform requirements* sooner than 1 November 2007.

1.4 G The ability to comply with the *common platform requirements* before 1 November 2007 does not apply to *SYSC* 9 (Record-keeping), *SYSC* 8.2 (Outsourcing of portfolio management for retail clients to a non-EEA State) or *SYSC* 8.3 (Guidance on outsourcing portfolio management for retail clients to a non-EEA State). All *firms* must continue to comply with the record-keeping requirements in *SYSC* 3.2.20R until 1 November 2007, when *SYSC* 9 will enter into force.

The decision to comply with the common platform requirements

1.5 R *SYSC* 4 to 7, *SYSC* 8.1 and *SYSC* 10 do not apply to a *firm* unless it decides to comply with them sooner than 1 November 2007.

1.6 R If a *firm* decides to comply with the *common platform requirements* in accordance with *SYSC* TP 1.5R:

(1) it must make a record of the date of the decision and the date from which it is to be effective; and

(2) subject to *SYSC* TP 1.7R below, from the effective date, it must comply with *SYSC* 4 to 7, *SYSC* 8.1 and *SYSC* 10, and *SYSC* 3 will not apply to it.

1.7 R The following provisions in *SYSC* 3 will continue to apply to a *firm* that decides to comply with the *common platform requirements* before the 1 November 2007:

(1) *SYSC* 3.2.23R, *SYSC* 3.2.24R, *SYSC* 3.2.26R and *SYSC* 3.2.28R to *SYSC* 3.2.35R in so far as *SYSC* 12.1.13R applies to it; and

(2) *SYSC* 3.2.20R to *SYSC* 3.2.22G.

1.8 G The purpose of *SYSC* TP 1.7R is to ensure the effective operation of the provisions on consolidated risk management processes and internal control mechanisms in relation to a *firm* that decides to comply with the *common platform requirements* before 1 November 2007.

1.9 G A decision by a *firm* to comply with the *common platform requirements* must be made in relation to all of the *common platform requirements*. The firm may not 'cherry-pick'.

Definitions in SYSC TP1 and the common platform requirements

1.10 R The terms *common platform firm* and *MiFID investment firm* have effect in *SYSC* TP1 and the *common platform requirements* as if *MiFID* applied generally from 1 January 2007.

To be inserted after SYSC 3

4 General organisational requirements

4.1 General requirements

4.1.1 R A *common platform firm* must have robust governance arrangements, which include a clear organisational structure with well defined, transparent and consistent lines of responsibility, effective processes to identify, manage, monitor and report the risks it is or might be exposed to, and internal control mechanisms, including sound administrative and accounting procedures and effective control and safeguard arrangements for information processing systems.

[Note**:** article 22(1) of the *Banking Consolidation Directive*, article 13(5) second paragraph of *MiFID*]

4.1.2 R The arrangements, processes and mechanisms referred to in *SYSC* 4.1.1R must be comprehensive and proportionate to the nature, scale and complexity of the *common platform firm's* activities and must take into account the specific technical criteria described in *SYSC* 4.1.7R, *SYSC* 5.1.7R and *SYSC* 7.

[Note**:** article 22(2) of the *Banking Consolidation Directive*]

4.1.3 R A *BIPRU firm* must ensure that its internal control mechanisms and administrative and accounting procedures permit the verification of its compliance with *rules* adopted in accordance with the *Capital Adequacy Directive* at all times.

[Note**:** article 35(1) final sentence of the *Capital Adequacy Directive*]

4.1.4 R A *common platform firm* must, taking into account the nature, scale and complexity of the business of the *firm*, and the nature and range of the *investment services and activities* undertaken in the course of that business:

(1) establish, implement and maintain decision-making procedures and an organisational structure which clearly and in a documented manner specifies reporting lines and allocates functions and responsibilities;

(2) establish, implement and maintain adequate internal control mechanisms designed to secure compliance with decisions and procedures at all levels of the *firm*; and

(3) establish, implement and maintain effective internal reporting and communication of information at all relevant levels of the *firm*.

[Note**:** articles 5(1) final paragraph, 5(1)(a), 5(1)(c) and 5(1)(e) of the *MiFID implementing Directive*]

4.1.5 R A *MiFID investment firm* must establish, implement and maintain systems

and procedures that are adequate to safeguard the security, integrity and confidentiality of information, taking into account the nature of the information in question.

[Note**:** article 5(2) of the *MiFID implementing Directive*]

Business continuity

4.1.6 R A *common platform firm* must take reasonable steps to ensure continuity and regularity in the performance of its *regulated activities*. To this end the *firm* must employ appropriate and proportionate systems, resources and procedures.

[Note**:** article 13(4) of *MiFID*]

4.1.7 R A *common platform firm* must establish, implement and maintain an adequate business continuity policy aimed at ensuring, in the case of an interruption to its systems and procedures, that any losses are limited, the preservation of essential data and functions, and the maintenance of its *regulated activities*, or, where that is not possible, the timely recovery of such data and functions and the timely resumption of its *regulated activities*.

[Note**:** article 5(3) of the *MiFID implementing Directive* and annex V paragraph 13 of the *Banking Consolidation Directive*]

4.1.8 G The matters dealt with in a business continuity policy should include:

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

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

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

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

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

(6) regular testing of the business continuity policy in an appropriate and proportionate manner in accordance with *SYSC* 4.1.10R.

Accounting policies

4.1.9 R A *common platform firm* must establish, implement and maintain accounting policies and procedures that enable it, at the request of the *FSA*, to deliver in a timely manner to the *FSA* financial reports which reflect a true and fair view of its financial position and which comply with all applicable accounting standards and rules.

[Note**:** article 5(4) of the *MiFID implementing Directive*]

Regular monitoring

4.1.10 R A *common platform firm* must monitor and, on a regular basis, evaluate the adequacy and effectiveness of its systems, internal control mechanisms and arrangements established in accordance with *SYSC* 4.1.4R to *SYSC* 4.1.9R and take appropriate measures to address any deficiencies.

[Note**:** article 5(5) of the *MiFID implementing Directive*]

Audit committee

4.1.11 G Depending on the nature, scale and complexity of its business, it may be appropriate for a *firm* to form an audit committee. An audit committee could typically examine management's process for ensuring the appropriateness and effectiveness of systems and controls, examine the arrangements made by management to ensure compliance with requirements and standards under the *regulatory system*, oversee the functioning of the internal audit function (if applicable) and provide an interface between management and external auditors. It should have an appropriate number of *non-executive directors* and it should have formal terms of reference.

4.2 Persons who effectively direct the business

4.2.1 R The *senior personnel* of a *common platform firm* must be of sufficiently good repute and sufficiently experienced as to ensure the sound and prudent management of the *firm*.

[Note**:** article 9(1) of *MiFID* and article 11(1) second paragraph of the *Banking Consolidation Directive*]

4.2.2 R A *common platform firm* must ensure that its management is undertaken by at least two persons meeting the requirements laid down in *SYSC* 4.2.1R.

[Note**:** article 9(4) first paragraph of *MiFID* and article 11(1) first paragraph of the *Banking Consolidation Directive*]

4.2.3 G In the case of a *body corporate*, the persons referred to in *SYSC* 4.2.2R should either be executive *directors* or persons granted executive powers by, and reporting immediately to, the *governing body*. In the case of a *partnership*, they should be active *partners*.

4.2.4 G At least two independent minds should be applied to both the formulation

and implementation of the policies of a *common platform firm*. Where a *common platform firm* nominates just two individuals to direct its business, the *FSA* will not regard them as both effectively directing the business where one of them makes some, albeit significant, decisions relating to only a few aspects of the business. Each should play a part in the decision-making process on all significant decisions. Both should demonstrate the qualities and application to influence strategy, day-to-day policy and its implementation. This does not require their day-to-day involvement in the execution and implementation of policy. It does, however, require involvement in strategy and general direction, as well as knowledge of, and influence on, the way in which strategy is being implemented through day-to-day policy.

4.2.5 G Where there are more than two individuals directing the business, the *FSA* does not regard it as necessary for all of these individuals to be involved in all decisions relating to the determination of strategy and general direction. However, at least two individuals should be involved in all such decisions. Both individuals' judgement should be engaged so that major errors leading to difficulties for the *firm* are less likely to occur. Similarly, each individual should have sufficient experience and knowledge of the business and the necessary personal qualities and skills to detect and resist any imprudence, dishonesty or other irregularities by the other individual. Where a single individual, whether a chief executive, managing *director* or otherwise, is particularly dominant in a *firm* this will raise doubts about whether *SYSC* 4.2.2R is met.

4.2.6 R If a *common platform firm*, other than a *credit institution*, is:

(1) a natural person; or

(2) a legal person managed by a single natural person;

it must have alternative arrangements in place which ensure sound and prudent management of the *firm*.

[Note**:** article 9(4) second paragraph of *MiFID*]

4.3 Responsibility of senior personnel

4.3.1 R A *MiFID investment firm*, when allocating functions internally, must ensure that *senior personnel* and, where appropriate, the *supervisory function*, are responsible for ensuring that the *firm* complies with its obligations under *MiFID*. In particular, *senior personnel* and, where appropriate, the *supervisory function* must assess and periodically review the effectiveness of the policies, arrangements and procedures put in place to comply with the *firm's* obligations under *MiFID* and take appropriate measures to address any deficiencies.

[Note**:** article 9(1) of the *MiFID implementing Directive*]

4.3.2 R A *MiFID investment firm*, must ensure:

(1) that its *senior personnel* receive on a frequent basis, and at least annually, written reports on the matters covered by *SYSC* 6.1.2R to 6.1.5R, *SYSC* 6.2.1R and *SYSC* 7.1.2R, *SYSC* 7.1.3R and *SYSC* 7.1.5R to *SYSC* 7.1.7R, indicating in particular whether the appropriate remedial measures have been taken in the event of any deficiencies; and

(2) the *supervisory function*, if any, must receive on a regular basis written reports on the same matters.

[Note**:** article 9(2) and article 9(3) of the *MiFID implementing Directive*]

4.3.3 G The *supervisory function* does not include a general meeting of the shareholders of a *common platform firm*, or equivalent bodies, but could involve, for example, a separate supervisory board within a two-tier board structure or the establishment of a non-executive committee of a single-tier board structure.

4.3.4 G *SYSC* 2, which sets out how certain functions in a firm should be allocated, does not affect the collective responsibility of the *senior personnel* of a *MiFID investment firm* under this section.

5 Employees, agents and other relevant persons

5.1 Skills, knowledge and expertise

5.1.1 R A *common platform firm* must employ personnel with the skills, knowledge and expertise necessary for the discharge of the responsibilities allocated to them.

[Note**:** article 5(1)(d) of the *MiFID implementing Directive*]

5.1.2 G A *firm's* systems and controls should enable it to satisfy itself of the suitability of anyone who acts for it. This includes assessing an individual's honesty and competence. This assessment should normally be made at the point of recruitment. An individual's honesty need not normally be revisited unless something happens to make a fresh look appropriate.

5.1.3 G Any assessment of an individual's suitability should take into account the level of responsibility that the individual will assume within the *firm*. The nature of this assessment will generally differ depending upon whether it takes place at the start of the individual's recruitment, at the end of the probationary period (if there is one) or subsequently.

5.1.4 G The *FSA*'s requirements on *firms* with respect to the competence of individuals are in the Training and Competence sourcebook (*TC*).

5.1.5 G The requirements on *firms* with respect to *approved persons* are in Part V of the *Act* (Performance of regulated activities) and *SUP* 10.

Segregation of functions

5.1.6 R A *common platform firm* must ensure that the performance of multiple functions by its *relevant persons* does not and is not likely to prevent those persons from discharging any particular functions soundly, honestly and professionally.

[Note**:** article 5(1)(g) of the *MiFID implementing Directive*]

5.1.7 R The *senior personnel* of a *common platform firm* must define arrangements concerning the segregation of duties within the *firm* and the prevention of conflicts of interest.

[Note**:** annex V paragraph 1 of the *Banking Consolidation Directive*]

5.1.8 G The effective segregation of duties is an important element in the *internal controls* of a *firm* in the *prudential context*. In particular, it helps to ensure that no one individual is completely free to commit a *firm*'s assets or incur liabilities on its behalf. Segregation can also help to ensure that a *firm's governing body* receives objective and accurate information on financial performance, the risks faced by the *firm* and the adequacy of its systems.

5.1.9 G A *common platform firm* should normally ensure that no single individual has unrestricted authority to do all of the following:

(1) initiate a transaction;

(2) bind the *firm*;

(3) make payments; and

(4) account for it.

5.1.10 G Where a *common platform firm* is unable to ensure the complete segregation of duties (for example, because it has a limited number of staff), it should ensure that there are adequate compensating controls in place (for example, frequent review of an area by relevant *senior managers*).

5.1.11 G Where a *common platform firm* outsources its internal audit function, it should take reasonable steps to ensure that every individual involved in the performance of this service is independent from the individuals who perform its external audit. This should not prevent services from being undertaken by a *firm's* external auditors provided that:

(1) the work is carried out under the supervision and management of the *firm's* own internal staff; and

(2) potential conflicts of interest between the provision of external audit services and the provision of internal audit are properly managed.

Awareness of procedures

5.1.12 R A *common platform firm* must ensure that its *relevant persons* are aware of the procedures which must be followed for the proper discharge of their responsibilities.

[Note**:** article 5(1)(b) of the *MiFID implementing Directive*]

General

5.1.13 R The systems, internal control mechanisms and arrangements established by a *firm* in accordance with this chapter must take into account the nature, scale and complexity of its business and the nature and range of *investment services and activities* undertaken in the course of that business.

[Note: article 5(1) final paragraph of the *MiFID implementing Directive*]

5.1.14 R A *common platform firm* must monitor and, on a regular basis, evaluate the adequacy and effectiveness of its systems, internal control mechanisms and arrangements established in accordance with this chapter, and take appropriate measures to address any deficiencies.

[Note: article 5(5) of the *MiFID implementing Directive*]

6 Compliance, internal audit and financial crime

6.1 Compliance

6.1.1 R A *common platform firm* must establish, implement and maintain adequate policies and procedures sufficient to ensure compliance of the *firm* including its managers, employees and *appointed representatives* with its obligations under the *regulatory system*.

[Note**:** article 13(2) of *MiFID*]

6.1.2 R A *common platform firm* must, taking in to account the nature, scale and complexity of its business, and the nature and range of *investment services and activities* undertaken in the course of that business, establish, implement and maintain adequate policies and procedures designed to detect any risk of failure by the *firm* to comply with its obligations under the *regulatory system*, as well as associated risks, and put in place adequate measures and procedures designed to minimise such risks and to enable the *FSA* to exercise its powers effectively under the *regulatory system* and to enable any other *competent authority* to exercise its powers effectively under *MiFID*.

[Note**:** article 6(1) of the *MiFID implementing Directive*]

6.1.3 R A *common platform firm* must maintain a permanent and effective compliance function which operates independently and which has the following responsibilities:

(1) to monitor and, on a regular basis, to assess the adequacy and effectiveness of the measures and procedures put in place in accordance with *SYSC* 6.1.2R, and the actions taken to address any deficiencies in the *firm*'s compliance with its obligations;

(2) to advise and assist the *relevant persons* responsible for carrying out *regulated activities* to comply with the *firm's* obligations under the *regulatory system*.

[Note: article 6(2) of the *MiFID implementing Directive*]

6.1.4 R In order to enable the compliance function to discharge its responsibilities properly and independently, a *common platform firm* must ensure that the following conditions are satisfied:

(1) the compliance function must have the necessary authority, resources, expertise and access to all relevant information;

(2) a compliance officer must be appointed and must be responsible for the compliance function and for any reporting as to compliance required by *SYSC* 4.3.2R;

(3) the *relevant persons* involved in the compliance functions must not be

involved in the performance of services or activities they monitor;

(4) the method of determining the remuneration of the *relevant persons* involved in the compliance function must not compromise their objectivity and must not be likely to do so.

[Note**:** article 6(3) first paragraph of the *MiFID implementing Directive*]

6.1.5 R A *common platform firm* need not comply with *SYSC* 6.1.4R(3) or *SYSC* 6.1.4R(4) if it is able to demonstrate that in view of the nature, scale and complexity of its business, and the nature and range of *investment services and activities*, the requirements under those *rules* are not proportionate and that its compliance function continues to be effective.

[Note**:** article 6(3) second paragraph of the *MiFID implementing Directive*]

6.2 Internal audit

6.2.1 R A *common platform firm* must, where appropriate and proportionate in view of the nature, scale and complexity of its business and the nature and range of *investment services and activities* undertaken in the course of that business, establish and maintain an internal audit function which is separate and independent from the other functions and activities of the *firm* and which has the following responsibilities:

(1) to establish, implement and maintain an audit plan to examine and evaluate the adequacy and effectiveness of the *firm's* systems, internal control mechanisms and arrangements;

(2) to issue recommendations based on the result of work carried out in accordance with (1);

(3) to verify compliance with those recommendations;

(4) to report in relation to internal audit matters in accordance with *SYSC* 4.3.2R.

[Note**:** article 8 of the *MiFID implementing Directive*]

6.3 Financial crime

6.3.1 R A *common platform firm* must ensure the policies and procedures established under *SYSC* 6.1.1R include systems and controls that:

(1) enable it to identify, assess, monitor and manage *money laundering* risk; and

(2) are comprehensive and proportionate to the nature, scale and complexity of its activities.

6.3.2 G "*Money laundering* risk" is the risk that a *firm* may be used to further *money laundering*. Failure by a *firm* to manage this risk effectively will increase the

risk to society of crime and terrorism.

6.3.3 R A *common platform firm* must carry out regular assessment of the adequacy of these systems and controls to ensure that it continues to comply with *SYSC* 6.3.1R.

6.3.4 G A *common platform firm* may also have separate obligations to comply with relevant legal requirements, including the Terrorism Act 2000, the Proceeds of Crime Act 2002 and the *Money Laundering Regulations*. *SYSC* 6.1.1R and *SYSC* 6.3.1R to *SYSC* 6.3.10G are not relevant for the purposes of regulation 3(3) of the *Money Laundering Regulations*, section 330(8) of the Proceeds of Crime Act 2002 or section 21A(6) of the Terrorism Act 2000.

6.3.5 G The *FSA*, when considering whether a breach of its *rules* on systems and controls against *money laundering* has occurred, will have regard to whether a *common platform firm* has followed relevant provisions in the guidance for the *United Kingdom* financial sector issued by the Joint Money Laundering Steering Group.

6.3.6 G In identifying its *money laundering* risk and in establishing the nature of these systems and controls, a *common platform firm* should consider a range of factors, including:

(1) its customer, product and activity profiles;

(2) its distribution channels;

(3) the complexity and volume of its transactions;

(4) its processes and systems; and

(5) its operating environment.

6.3.7 G A *common platform firm* should ensure that the systems and controls include:

(1) appropriate training for its employees in relation to *money laundering*;

(2) appropriate provision of information to its *governing body* and senior management, including a report at least annually by that *firm's money laundering reporting officer* (*MLRO*) on the operation and effectiveness of those systems and controls;

(3) appropriate documentation of its risk management policies and risk profile in relation to *money laundering*, including documentation of its application of those policies (see *SYSC* 9);

(4) appropriate measures to ensure that *money laundering* risk is taken into account in its day-to-day operation, including in relation to:

(a) the development of new products;

(b) the taking-on of new customers; and

(c) changes in its business profile; and

(5) appropriate measures to ensure that procedures for identification of new customers do not unreasonably deny access to its services to potential customers who cannot reasonably be expected to produce detailed evidence of identity.

6.3.8 R A *common platform firm* must allocate to a *director* or *senior manager* (who may also be the *money laundering reporting officer*) overall responsibility within the *firm* for the establishment and maintenance of effective anti-*money laundering* systems and controls.

The money laundering reporting officer

6.3.9 R A *common platform firm* must:

(1) appoint an individual as *MLRO*, with responsibility for oversight of its compliance with the *FSA's rules* on systems and controls against *money laundering*; and

(2) ensure that its *MLRO* has a level of authority and independence within the *firm* and access to resources and information sufficient to enable him to carry out that responsibility.

6.3.10 G The job of the *MLRO* within a *firm* is to act as the focal point for all activity within the *firm* relating to anti-*money laundering*. The *FSA* expects that a *firm's MLRO* will be based in the *United Kingdom*.

7 Risk control

7.1 Risk control

7.1.1 G *SYSC* 4.1.1R requires a *common platform firm* to have effective processes to identify, manage, monitor and report the risks it is or might be exposed to.

7.1.2 R A *common platform firm* must establish, implement and maintain adequate risk management policies and procedures, including effective procedures for risk assessment, which identify the risks relating to the *firm's* activities, processes and systems, and where appropriate, set the level of risk tolerated by the *firm*.

[Note: article 7(1)(a) of the *MiFID implementing Directive*, article 13(5) second paragraph of *MiFID*]

7.1.3 R A *common platform firm* must adopt effective arrangements, processes and mechanisms to manage the risk relating to the *firm's* activities, processes and systems, in light of that level of risk tolerance.

[Note: article 7(1)(b) of the *MiFID implementing Directive*]

7.1.4 R The *senior personnel* of a *common platform firm* must approve and periodically review the strategies and policies for taking up, managing, monitoring and mitigating the risks the *firm* is or might be exposed to, including those posed by the macroeconomic environment in which it operates in relation to the status of the business cycle.

[Note: annex V paragraph 2 of the *Banking Consolidation Directive*]

7.1.5 R A *common platform firm* must monitor the following:

(1) the adequacy and effectiveness of the *firm's* risk management policies and procedures;

(2) the level of compliance by the *firm* and its *relevant persons* with the arrangements, processes and mechanisms adopted in accordance with *SYSC* 7.1.3R;

(3) the adequacy and effectiveness of measures taken to address any deficiencies in those policies, procedures, arrangements, processes and mechanisms, including failures by the *relevant persons* to comply with such arrangements or processes and mechanisms or follow such policies and procedures.

[Note: article 7(1)(c) of the *MiFID implementing Directive*]

7.1.6 R A *common platform firm* must, where appropriate and proportionate in view of the nature, scale and complexity of its business and the nature and range of the *investment services and activities* undertaken in the course of that business, establish and maintain a risk management function that operates

independently and carries out the following tasks:

(1) implementation of the policies and procedures referred to in *SYSC* 7.1.2R to *SYSC* 7.1.5R; and

(2) provision of reports and advice to *senior personnel* in accordance with *SYSC* 4.3.2R.

[Note: *MiFID implementing Directive* article 7(2) first paragraph]

7.1.7 R Where a *common platform firm* is not required under *SYSC* 7.1.6R to maintain a risk management function that functions independently, it must nevertheless be able to demonstrate that the policies and procedures which it has adopted in accordance with *SYSC* 7.1.2R to *SYSC* 7.1.5R satisfy the requirements of those *rules* and are consistently effective.

[Note: article 7(2) second paragraph of the *MiFID implementing Directive*]

7.1.8 G *SYSC* 4.1.3R requires a *BIPRU firm* to ensure that its internal control mechanisms and administrative and accounting procedures permit the verification of its compliance with *rules* adopted in accordance with the *Capital Adequacy Directive* at all times. In complying with this obligation, a *BIPRU firm* should document the organisation and responsibilities of its risk management function and it should document its risk management framework setting out how the risks in the business are identified, measured, monitored and controlled.

Credit and counterparty risk

7.1.9 R A *BIPRU firm* must base credit-granting on sound and well-defined criteria and clearly establish the process for approving, amending, renewing, and re-financing credits.

[Note: annex V paragraph 3 of the *Banking Consolidation Directive*]

7.1.10 R A *BIPRU firm* must operate through effective systems the ongoing administration and monitoring of its various credit risk-bearing portfolios and exposures, including for identifying and managing problem credits and for making adequate value adjustments and provisions.

[Note: annex V paragraph 4 of the *Banking Consolidation Directive*]

7.1.11 R A *BIPRU firm* must adequately diversify credit portfolios given its target market and overall credit strategy.

[Note: annex V paragraph 5 of the *Banking Consolidation Directive*]

7.1.12 G The documentation maintained by a *BIPRU firm* under *SYSC* 4.1.3R should include its policy for credit risk, including its risk appetite and provisioning policy and should describe how it measures, monitors and controls that risk. This should include descriptions of the systems used to ensure that the

policy is correctly implemented.

Residual risk

7.1.13 R A *BIPRU firm* must address and control by means of written policies and procedures the risk that recognised credit risk mitigation techniques used by it prove less effective than expected.

[Note: annex V paragraph 6 of the *Banking Consolidation Directive*]

Market risk

7.1.14 R A *BIPRU firm* must implement policies and processes for the measurement and management of all material sources and effects of market risks.

[Note: annex V paragraph 10 of the *Banking Consolidation Directive*]

Interest rate risk

7.1.15 R A *BIPRU firm* must implement systems to evaluate and manage the risk arsing from potential changes in interest rates as they affect a *BIPRU firm's* non-trading activities.

[Note: annex V paragraph 11 of the *Banking Consolidation Directive*]

Operational risk

7.1.16 R A *BIPRU firm* must implement policies and processes to evaluate and manage the exposure to operational risk, including to low-frequency high severity events. Without prejudice to the definition of *operational risk*, *BIPRU firms* must articulate what constitutes operational risk for the purposes of those policies and procedures.

[Note: annex V paragraph 12 of the *Banking Consolidation Directive*]

8 Outsourcing

8.1 General outsourcing requirements

8.1.1 R A *common platform firm* must:

(1) when relying on a third party for the performance of operational functions which are critical for the performance of *regulated activities*, *listed activities* or *ancillary services* (in this chapter "relevant services and activities") on a continuous and satisfactory basis, ensure that it takes reasonable steps to avoid undue additional operational risk;

(2) not undertake the o*utsourcing* of important operational functions in such a way as to impair materially:

(a) the quality of its internal control; and

(b) the ability of the *FSA* to monitor the *firm's* compliance with all obligations under the *regulatory system* and, if different, of a *competent authority* to monitor the *firm's* compliance with all obligations under *MiFID*.

[Note**:** article 13(5) first paragraph of *MiFID*]

8.1.2 G The application of *SYSC* 8.1 to relevant services and activities (see *SYSC* 8.1.1R(1)) is limited by *SYSC* 1.3 (Application of the common platform requirements).

8.1.3 G *SYSC* 4.1.1R requires a *common platform firm* to have effective processes to identify, manage, monitor and report risks and internal control mechanisms. Except in relation to those functions described in *SYSC* 8.1.5R, where a *firm* relies on a third party for the performance of operational functions which are not critical or important for the performance of relevant services and activities (see *SYSC* 8.1.1R(1)) on a continuous and satisfactory basis, it should take into account, in a manner that is proportionate given the nature, scale and complexity of the *outsourcing*, the *rules* in this section in complying with that requirement.

8.1.4 R For the purposes of this chapter an operational function is regarded as critical or important if a defect or failure in its performance would materially impair the continuing compliance of a *common platform firm* with the conditions and obligations of its *authorisation* or its other obligations under the *regulatory system*, or its financial performance, or the soundness or the continuity of its relevant services and activities.

[Note**:** article 13(1) of the *MiFID implementing Directive*]

8.1.5 R Without prejudice to the status of any other function, the following functions will not be considered as critical or important for the purposes of

this chapter:

(1) the provision to the *firm* of advisory services, and other services which do not form part of the relevant services and activities of the *firm*, including the provision of legal advice to the *firm*, the training of personnel of the *firm*, billing services and the security of the *firm's* premises and personnel;

(2) the purchase of standardised services, including market information services and the provision of price feeds.

[Note**:** article 13(2) of the *MiFID implementing Directive*]

8.1.6 R If a *common platform firm outsources* critical or important operational functions or any relevant services and activities, it remains fully responsible for discharging all of its obligations under the *regulatory system* and must comply, in particular, with the following conditions:

(1) the *outsourcing* must not result in the delegation by *senior personnel* of their responsibility;

(2) the relationship and obligations of the *firm* towards its *clients* under the *regulatory system* must not be altered;

(3) the conditions with which the *firm* must comply in order to be *authorised*, and to remain so, must not be undermined;

(4) none of the other conditions subject to which the *firm's authorisation* was granted must be removed or modified.

[Note**:** article 14(1) of the *MiFID implementing Directive*]

8.1.7 R A *common platform firm* must exercise due skill and care and diligence when entering into, managing or terminating any arrangement for the *outsourcing* to a service provider of critical or important operational functions or of any relevant services and activities.

[Note**:** article 14(2) first paragraph of the *MiFID implementing Directive*]

8.1.8 R A *common platform firm* must in particular take the necessary steps to ensure that the following conditions are satisfied:

(1) the service provider must have the ability, capacity, and any *authorisation* required by law to perform the *outsourced* functions, services or activities reliably and professionally;

(2) the service provider must carry out the *outsourced* services effectively, and to this end the *firm* must establish methods for assessing the standard of performance of the service provider;

(3) the service provider must properly supervise the carrying out of the *outsourced* functions, and adequately manage the risks associated

with the *outsourcing*;

(4) appropriate action must be taken if it appears that the service provider may not be carrying out the functions effectively and in compliance with applicable laws and regulatory requirements;

(5) the *firm* must retain the necessary expertise to supervise the *outsourced* functions effectively and manage the risks associated with the *outsourcing* and must manage those risks and must supervise those functions and manage those risks;

(6) the service provider must disclose to the *firm* any development that may have a material impact on its ability to carry out the *outsourced* functions effectively and in compliance with applicable laws and regulatory requirements;

(7) the *firm* must be able to terminate the arrangement for the *outsourcing* where necessary without detriment to the continuity and quality of its provision of services to *clients*;

(8) the service provider must co-operate with the *FSA* and any other relevant *competent authority* in connection with the *outsourced* activities;

(9) the *firm*, it auditors, the *FSA* and any other relevant *competent authority* must have effective access to data related to the *outsourced* activities, as well as to the business premises of the service provider; and the *FSA* and any other relevant *competent authority* must be able to exercise those rights of access;

(10) the service provider must protect any confidential information relating to the *firm* and its *clients*;

(11) the *firm* and the service provider must establish, implement and maintain a contingency plan for disaster recovery and periodic testing of backup facilities where that is necessary having regard to the function, service or activity that has been *outsourced*.

[Note**:** article 14(2) second paragraph of the *MiFID implementing Directive*]

8.1.9 R A *common platform firm* must ensure that the respective rights and obligations of the *firm* and of the service provider are clearly allocated and set out in a written agreement.

[Note**:** article 14(3) of the *MiFID implementing Directive*]

8.1.10 R If a *common platform firm* and the service provider are members of the same *group*, the *firm* may, for the purpose of complying with *SYSC* 8.1.7R to *SYSC* 8.1.11R and *SYSC* 8.2 and *SYSC* 8.3, take into account the extent to which the *common platform firm controls* the service provider or has the

ability to influence its actions.

[Note**:** article 14(4) of the *MiFID implementing Directive*]

8.1.11 R A *common platform firm* must make available on request to the *FSA* and any other relevant *competent authority* all information necessary to enable the *FSA* and any other relevant *competent authority* to supervise the compliance of the performance of the *outsourced* activities with the requirements of the *regulatory system*.

[Note**:** article 14(5) of the *MiFID implementing Directive*]

8.1.12 G As *SUP* 15.3.8G explains, a *common platform firm* should notify the *FSA* when it intends to rely on a third party for the performance of operational functions which are critical or important for the performance of relevant services and activities on a continuous and satisfactory basis.

[Note**:** recital 20 of the *MiFID implementing Directive*]

To be inserted after SYSC 9

10.1 Conflicts of interest

Application

10.1.1 R This section applies to a *common platform firm* which provides services to its *clients* in the course of carrying on *regulated activities* or *ancillary activities*.

Requirements only apply if a service is provided

10.1.2 G The requirements in this section only apply where a service is provided by a *common platform firm*. The status of the *client* to whom the service is provided (as a *retail client*, *professional client* or *eligible counterparty*) is irrelevant for this purpose.

[Note: recital 25 of *MiFID implementing Directive*]

Identifying conflicts

10.1.3 R A *common platform firm* must take all reasonable steps to identify conflicts of interest between:

(1) the *firm*, including its managers, employees, *appointed representatives* or *tied agents*, or any *person* directly or indirectly linked to them by *control*, and a *client* of the *firm*; or

(2) one *client* of the *firm* and another *client*;

that arise, or may arise, in the course of the *firm* providing any service referred to in *SYSC* 10.1.1R.

[Note: article 18(1) of *MiFID*]

Types of conflicts

10.1.4 R For the purposes of identifying the types of conflict of interest that arise, or may arise, in the course of providing a service and whose existence may entail a material risk of damage to the interests of a *client*, a *common platform firm* must take into account, as a minimum, whether the *firm* or a *relevant person*, or a *person* directly or indirectly linked by *control* to the *firm*:

(1) is likely to make a financial gain, or avoid a financial loss, at the expense of the *client*;

(2) has an interest in the outcome of a service provided to the *client* or of a transaction carried out on behalf of the *client*, which is distinct from the *client*'s interest in that outcome;

(3) has a financial or other incentive to favour the interest of another *client* or group of *clients* over the interests of the *client*;

(4) carries on the same business as the *client*; or

(5) receives or will receive from a *person* other than the *client* an inducement in relation to a service provided to the *client*, in the form of monies, goods or services, other than the standard commission or fee for that service.

The conflict of interest may result from the *firm* or *person* providing a service referred to in *SYSC* 10.1.1R or engaging in any other activity.

[Note: article 21 of *MiFID implementing Directive*]

10.1.5 G The circumstances which should be treated as giving rise to a conflict of interest should cover cases where there is a conflict between the interests of the *firm* or certain *persons* connected to the *firm* or the *firm's group* and the duty the *firm* owes to a *client*; or between the differing interests of two or more of its *clients*, to whom the *firm* owes in each case a duty. It is not enough that the *firm* may gain a benefit if there is not also a possible disadvantage to a *client*, or that one *client* to whom the *firm* owes a duty may make a gain or avoid a loss without there being a concomitant possible loss to another such *client*.

[Note: Recital 24 of *MiFID implementing Directive*]

Record of conflicts

10.1.6 R A *common platform firm* must keep and regularly update a record of the kinds of service or activity carried out by or on behalf of the *firm* in which a conflict of interest entailing a material risk of damage to the interests of one or more *clients* has arisen or, in the case of an ongoing service or activity, may arise.

[Note: article 23 of *MiFID implementing Directive*]

Managing conflicts

10.1.7 R A *common platform firm* must maintain and operate effective organisational and administrative arrangements with a view to taking all reasonable steps to prevent conflicts of interest as defined in *SYSC* 10.1.3R from constituting or giving rise to a material risk of damage to the interests of its *clients*.

[Note: article 13(3) of *MiFID*]

Disclosure of conflicts

10.1.8 R (1) If arrangements made by a *common platform firm* under *SYSC* 10.1.7R to manage conflicts of interest are not sufficient to ensure, with reasonable confidence, that risks of damage to the interests of a *client* will be prevented, the *firm* must clearly disclose the general

nature and/or sources of conflicts of interest to the *client* before undertaking business for the *client*.

(2) The disclosure must:

(a) be made in a *durable medium*; and

(b) include sufficient detail, taking into account the nature of the *client*, to enable that *client* to take an informed decision with respect to the service in the context of which the conflict of interest arises.

[Note: article 18(2) of *MiFID* and article 22(4) of *MiFID implementing Directive*]

10.1.9 G *Common platform firms* should aim to identify and manage the conflicts of interest arising in relation to their various business lines and their *group's* activities under a comprehensive *conflicts of interest policy*. In particular, the disclosure of conflicts of interest by a *firm* should not exempt it from the obligation to maintain and operate the effective organisational and administrative arrangements under *SYSC* 10.1.7R. While disclosure of specific conflicts of interest is required by *SYSC* 10.1.8R, an over-reliance on disclosure without adequate consideration as to how conflicts may appropriately be managed is not permitted.

[Note: Recital 27 of *MiFID implementing Directive*]

Conflicts policy

10.1.10 R (1) A *common platform firm* must establish, implement and maintain an effective conflicts of interest policy that is set out in writing and is appropriate to the size and organisation of the *firm* and the nature, scale and complexity of its business.

(2) Where the *common platform firm* is a member of a *group*, the policy must also take into account any circumstances, of which the *firm* is or should be aware, which may give rise to a conflict of interest arising as a result of the structure and business activities of other members of the *group*.

[Note: article 22(1) of *MiFID implementing Directive*]

Contents of policy

10.1.11 R (1) The *conflicts of interest policy* must include the following content:

(a) it must identify in accordance with *SYSC* 10.1.3R and *SYSC* 10.1.4R, by reference to the specific services and activities carried out by or on behalf of the *common platform firm*, the circumstances which constitute or may give rise to a conflict of interest entailing a material risk of damage to the interests

of one or more *clients*; and

(b) it must specify procedures to be followed and measures to be adopted in order to manage such conflicts.

(2) The procedures and measures provided for in paragraph (1)(b) must:

(a) be designed to ensure that *relevant person*s engaged in different business activities involving a conflict of interest of the kind specified in paragraph (1)(a) carry on those activities at a level of independence appropriate to the size and activities of the *common platform firm* and of the *group* to which it belongs, and to the materiality of the risk of damage to the interests of *clients*; and

(b) include such of the following as are necessary and appropriate for the *common platform firm* to ensure the requisite degree of independence:

(i) effective procedures to prevent or control the exchange of information between *relevant persons* engaged in activities involving a risk of a conflict of interest where the exchange of that information may harm the interests of one or more *clients*;

(ii) the separate supervision of *relevant persons* whose principal functions involve carrying out activities on behalf of, or providing services to, *clients* whose interests may conflict, or who otherwise represent different interests that may conflict, including those of the *firm*;

(iii) the removal of any direct link between the remuneration of *relevant person*s principally engaged in one activity and the remuneration of, or revenues generated by, different *relevant person*s principally engaged in another activity, where a conflict of interest may arise in relation to those activities;

(iv) measures to prevent or limit any *person* from exercising inappropriate influence over the way in which a *relevant person* carries out services or activities; and

(v) measures to prevent or control the simultaneous or sequential involvement of a *relevant person* in separate services or activities where such involvement may impair the proper management of conflicts of interest.

(3) If the adoption or the practice of one or more of those measures and

procedures does not ensure the requisite level of independence, a *common platform firm* must adopt such alternative or additional measures and procedures as are necessary and appropriate for those purposes.

[Note: article 22(2) and (3) of *MiFID implementing Directive*]

10.1.12 G In drawing up a *conflicts of interest policy* which identifies circumstances which constitute or may give rise to a conflict of interest, a *common platform firm* should pay special attention to the activities of investment research and advice, proprietary trading, portfolio management and corporate finance business, including underwriting or selling in an offering of securities and advising on mergers and acquisitions. In particular, such special attention is appropriate where the *firm* or a *person* directly or indirectly linked by *control* to the *firm* performs a combination of two or more of those activities.

[Note: Recital 26 of *MiFID implementing Directive*]

Corporate finance

10.1.13 G This section is relevant to the management of a *securities* offering by a *common platform firm.*

10.1.14 G A *common platform firm* will wish to note that when carrying on a mandate to manage an offering of *securities*, the *firm's* duty for that business is to its corporate finance *client* (in many cases, the corporate issuer or seller of the relevant *securities*), but that its responsibilities to provide services to its investment *clients* are unchanged.

10.1.15 G Measures that a *common platform firm* might wish to consider in drawing up its *conflicts of interest policy* in relation to the management of an offering of *securities* include:

(1) at an early stage agreeing with its corporate finance *client* relevant aspects of the offering process such as the process the *firm* proposes to follow in order to determine what recommendations it will make about allocations for the offering; how the target investor group will be identified; how recommendations on allocation and pricing will be prepared; and whether the *firm* might place *securities* with its investment *clients* or with its own proprietary book, or with an associate, and how conflicts arising might be managed; and

(2) agreeing allocation and pricing objectives with the corporate finance *client*; inviting the corporate finance *client* to participate actively in the allocation process; making the initial recommendation for allocation to *retail clients* of the *firm* as a single block and not on a named basis; having internal arrangements under which senior personnel responsible for providing services to *retail clients* make the initial allocation recommendations for allocation to *retail clients* of the *firm*; and disclosing to the *issuer* details of the allocations

actually made.

[Note: The provisions in *SYSC* 10.1 also implement *BCD* article 22 and *BCD* Annex V paragraph 1]

10.2 Chinese walls

Application

10.2.1 R This section applies to a *common platform firm*.

Control of information

10.2.2 R (1) When a *common platform firm* establishes and maintains a *Chinese wall* (that is, an arrangement that requires information held by a *person* in the course of carrying on one part of the business to be withheld from, or not to be used for, *persons* with or for whom it acts in the course of carrying on another part of its business) it may:

(a) withhold or not use the information held; and

(b) for that purpose, permit *persons* employed in the first part of its business to withhold the information held from those employed in that other part of the business;

but only to the extent that the business of one of those parts involves the carrying on of *regulated activities* or *ancillary activities*.

(2) Information may also be withheld or not used by a *common platform firm* when this is required by an established arrangement maintained between different parts of the business (of any kind) in the same *group*. This provision does not affect any requirement to transmit or use information that may arise apart from the *rules* in *COB* or *COBS*.

(3) For the purpose of this *rule*, "maintains" includes taking reasonable steps to ensure that the arrangements remain effective and are adequately monitored, and must be interpreted accordingly.

(4) For the purposes of section 118A(5)(a) of the *Act*, behaviour conforming with paragraph (1) does not amount to market abuse.

Effect of rules

10.2.3 G *SYSC* 10.2.2R is made under section 147 of the *Act* (Control of information rules). It has the following effect:

(1) acting in conformity with *SYSC* 10.2.2R(1) provides a defence against proceedings brought under section 397(2) or (3) of the *Act* (Misleading statements and practices) – see sections 397(4) and (5)(c);

(2) behaviour in conformity with *SYSC* 10.2.2R(1) does not amount to *market abuse* (see *SYSC* 10.2.2R(4)); and

(3) acting in conformity with *SYSC* 10.2.2R(1) provides a defence for a firm against *FSA* enforcement action, or an action for damages under

section 150 of the *Act*, based on a breach of a relevant requirement to disclose or use this information.

Attribution of knowledge

10.2.4 R When any of the *rules* of *COB*, *COBS* or *CASS* apply to a *common platform firm* that acts with knowledge, the *firm* will not be taken to act with knowledge for the purposes of that *rule* if none of the relevant individuals involved on behalf of the *firm* acts with that knowledge as a result of arrangements established under *SYSC* 10.2.2R.

10.2.5 G When a *common platform firm* manages a conflict of interest using the arrangements in *SYSC* 10.2.2R which take the form of a *Chinese wall*, individuals on the other side of the wall will not be regarded as being in possession of knowledge denied to them as a result of the *Chinese wall*.

Annex C
Senior Management Arrangements, Systems and Controls Handbook (SYSC)

In this Annex, the place where the text is being inserted is indicated and the text is not underlined.

11 Liquidity risk systems and controls

11.1 Application

11.1.1 R *SYSC* 11 applies to:

(1) an *insurer*, unless it is an *EEA deposit insurer* or a *Swiss general insurer*;

(2) a *BIPRU firm*;

(3) an *incoming EEA firm* which:

(a) is a *full BCD credit institution*; and

(b) has a *branch* in the *United Kingdom*;

(4) a *third country BIPRU firm* which:

(a) is a *bank*; and

(b) has a *branch* in the *United Kingdom*.

[Note**:** first paragraph of article 41 of the *Banking Consolidation Directive*]

11.1.2 R If this chapter applies because the *firm* has a *branch* in the *United Kingdom* (see *SYSC* 11.1.1R(3) or *SYSC* 11.1.1R(4)), *SYSC* 11 applies only with respect to the *branch*.

11.1.3 R *SYSC* 11 applies to an *incoming EEA firm* only to the extent that the relevant matter is not reserved by the relevant *Single Market Directive* to the *firm's Home State regulator*.

11.1.4 R *SYSC* 11 does not apply to:

(1) a *non-directive friendly society*; or

(2) a *UCITS qualifier*; or

(3) an *ICVC*; or

(4) an *incoming EEA firm* (unless it has a *branch* in the *United Kingdom* - see *SYSC* 11.1.1R(3)); or

(5) an *incoming Treaty firm*.

11.1.5 R (1) *SYSC* 11.1.11R and *SYSC* 11.1.12R apply only to a *BIPRU firm*

(2) *SYSC* 11.1.26G to *SYSC* 11.1.32G do not apply to *insurers*.

11.1.6 R If a *firm* carries on:

(1) *long-term insurance business*; and

(2) *general insurance business*;

SYSC 11 applies separately to each type of business.

Purpose

11.1.7 G The purpose of *SYSC* 11 is to amplify *GENPRU* and *SYSC* in their specific application to *liquidity risk* and, in so doing, to indicate minimum standards for systems and controls in respect of that risk.

11.1.8 G Appropriate systems and controls for the management of *liquidity risk* will vary with the scale, nature and complexity of the *firm's* activities. Most of the material in *SYSC* 11 is, therefore, *guidance*. *SYSC* 11 lays out some of the main issues that the *FSA* expects a *firm* to consider in relation to *liquidity risk*. A *firm* should assess the appropriateness of any particular item of *guidance* 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.

11.1.9 G *SYSC* 11 addresses the need to have appropriate systems and controls to deal both with liquidity management issues under normal market conditions, and with stressed or extreme situations resulting from either general market turbulence or *firm*-specific difficulties.

11.1.10 G *SYSC* 11.1.11R and *SYSC* 11.1.12R implement the specific *liquidity risk* requirements of the *BCD*.

Requirements

11.1.11 R A *BIPRU firm* must have policies and processes for the measurement and management of its net funding position and requirements on an ongoing and forward looking basis. Alternative scenarios must be considered and the assumptions underpinning decisions concerning the net funding position must be reviewed regularly.

[Note**:** annex V paragraph 14 of the *Banking Consolidation Directive*]

11.1.12 R A *BIPRU firm* must have contingency plans in place to deal with liquidity crises.

[Note**:** annex V paragraph 15 of the *Banking Consolidation Directive*]

11.1.13 G An *insurer* is also required to comply with the requirements in relation to

liquidity risk set out in *INSPRU* 4.1.

11.1.14 G *SYSC* 4.1.1R requires a *BIPRU firm* to have effective processes to identify, manage, monitor and report the risks it is or might be exposed to. A *BIPRU firm* is required by *SYSC* 7.1.2R to establish, implement and maintain adequate risk management policies and procedures, including effective procedures for risk assessment. *Liquidity risk* is one of the risks covered by both of those requirements.

11.1.15 G A *UK bank*, a *branch* of an *EEA bank* and a *branch* of an *overseas bank* is required in *IPRU(BANK)* GN 3.4.3R to set out its policy on the management of its liquidity. *Guidance* on a bank's liquidity policy statement is given in *IPRU(BANK)* LM Section 10. *Guidance* on a bank's management of *liquidity risk* is given in *IPRU(BANK)* LM Sections 2 and 9.

11.1.16 G A *building society* is required by *IPRU(BSOC)* 5.2.7R to maintain a board-approved policy statement on liquidity. *Guidance* on a *building society's* liquidity policy statement is given in *IPRU(BSOC)* 5.2.8G and *IPRU(BSOC)* Annex 5B. *Guidance* on a *building society's* management of *liquidity risk* is given in *IPRU(BSOC)* Sections 5.3 to 5.8.

11.1.17 G High level requirements in relation to carrying out stress testing and scenario analysis are set out in *GENPRU* 1.2. In particular, *GENPRU* 1.2.42R requires a *firm* to carry out appropriate stress testing and scenario analysis. *SYSC* 11 gives *guidance* in relation to these tests in the case of *liquidity risk.*

Stress testing and scenario analysis

11.1.18 G The effect of *GENPRU* 1.2.30R, *GENPRU* 1.2.34R, *GENPRU* 1.2.37R(1) and *GENPRU* 1.2.42R is that, for the purposes of determining the adequacy of its overall financial resources, a *firm* must carry out appropriate stress testing and scenario analysis, including taking reasonable steps to identify an appropriate range of realistic adverse circumstances and events in which *liquidity risk* might occur or crystallise.

11.1.19 G *GENPRU* 1.2.40G and *GENPRU* 1.2.62G to *GENPRU* 1.2.78G give *guidance* on stress testing and scenario analysis, including on how to choose appropriate scenarios, but the precise scenarios that a *firm* chooses to use will depend on the nature of its activities. For the purposes of testing *liquidity risk*, however, a *firm* should normally consider scenarios based on varying degrees of stress and both *firm*-specific and market-wide difficulties. In developing any scenario of extreme market-wide stress that may pose systemic risk, it may be appropriate for a *firm* to make assumptions about the likelihood and nature of central bank intervention.

11.1.20 G A *firm* should review frequently the assumptions used in stress testing scenarios to gain assurance that they continue to be appropriate.

11.1.21 E (1) A scenario analysis in relation to *liquidity risk* required under *GENPRU* 1.2.42R should include a cash-flow projection for each

scenario tested, based on reasonable estimates of the impact (both on and off balance sheet) of that scenario on the *firm's* funding needs and sources.

(2) Contravention of (1) may be relied on as tending to establish contravention of *GENPRU* 1.2.42R.

11.1.22 G In identifying the possible on and off balance sheet impact referred to in *SYSC* 11.1.21E(1), a *firm* may take into account:

(1) possible changes in the market's perception of the *firm* and the effects that this might have on the *firm's* access to the markets, including:

(a) (where the *firm* funds its holdings of assets in one currency with liabilities in another) access to foreign exchange markets, particularly in less frequently traded currencies;

(b) access to secured funding, including by way of repo transactions; and

(c) the extent to which the *firm* may rely on committed facilities made available to it;

(2) (if applicable) the possible effect of each scenario analysed on currencies whose exchange rates are currently pegged or fixed; and

(3) that:

(a) general market turbulence may trigger a substantial increase in the extent to which *persons* exercise rights against the *firm* under off balance sheet instruments to which the *firm* is party;

(b) access to *OTC derivative* and foreign exchange markets are sensitive to credit-ratings;

(c) the scenario may involve the triggering of early amortisation in asset securitisation transactions with which the *firm* has a connection; and

(d) its ability to securitise assets may be reduced.

Contingency funding plans

11.1.23 G *GENPRU* 1.2.26R states that a *firm* must at all times maintain overall financial resources adequate to ensure that there is no significant risk that its liabilities cannot be met as they fall due. *GENPRU* 1.2.42R(1)(b) provides that for the purposes of determining the adequacy of its overall financial resources, a *firm* must estimate the financial resources it would need in each of the circumstances and events considered in carrying out its stress testing and scenario analysis in order to, inter alia, meet its liabilities as they fall due.

11.1.24 E (1) A *firm* should have an adequately documented *contingency funding plan* for taking action to ensure, so far as it can, that, in each of the scenarios analysed under *GENPRU* 1.2.42R(1)(b), it would still have sufficient liquid financial resources to meet liabilities as they fall due.

(2) The *contingency funding plan* should cover what events or circumstances will lead the *firm* to put into action any part of the plan.

(3) The *contingency funding plan* of a *firm* described in *SYSC* 11.1.1R(2) to *SYSC* 11.1.1R(4) should cover the extent to which the actions in (1) include:

(a) selling, using as *collateral* in secured funding (including repo), or securitising, its assets;

(b) otherwise reducing its assets;

(c) modifying the structure of its liabilities or increasing its liabilities; and

(d) the use of committed facilities.

(4) A *firm*'s *contingency funding plan* should, where relevant, take account of the impact of stressed market conditions on:

(a) the behaviour of any credit-sensitive liabilities it has; and

(b) its ability to securitise assets.

(5) A *firm*'s *contingency funding plan* should contain administrative policies and procedures that will enable the *firm* to manage the plan's implementation effectively, including:

(a) the responsibilities of senior management;

(b) names and contact details of members of the team responsible for implementing the *contingency funding plan*;

(c) where, geographically, team members will be assigned;

(d) who within the team is responsible for contact with head office (if appropriate), analysts, investors, external auditors, press, significant *client's*, regulators, lawyers and others; and

(e) mechanisms that enable senior management and the *governing body* to receive management information that is both relevant and timely.

(6) Contravention of any of (1) to (5) may be relied upon as tending to

establish contravention of *GENPRU* 1.2.30R(2)(c).

Documentation

11.1.25 G *GENPRU* 1.2.60R requires a *firm* to document its assessment of the adequacy of its liquidity financial resources, how it intends to deal with those risks, and details of the stress tests and scenario analyses carried out and the resulting financial resources estimated to be required. Accordingly, a *firm* should document both its stress testing and scenario analysis (see *SYSC* 11.1.18G) and its *contingency funding plan* (see *SYSC* 11.1.23G).

Management information systems

11.1.26 G A *firm* should have adequate information systems for controlling and reporting *liquidity risk*. The management information system should be used to check for compliance with the *firm's* established policies, procedures and limits.

11.1.27 G Reports on *liquidity risk* should be provided on a timely basis to the *firm's governing body*, senior management and other appropriate personnel. The appropriate content and format of reports depends on a *firm's* liquidity management practices and the nature, scale and complexity of the *firm's* business. Reports to the *firm's governing body* may be less detailed and less frequent than reports to senior management with responsibility for managing *liquidity risk*.

11.1.28 G The *FSA* would expect management information to normally contain the following:

(1) a cash-flow or funding gap report;

(2) a funding maturity schedule;

(3) a list of large providers of funding; and

(4) a limit monitoring and exception report.

11.1.29 G When considering what else might be included in *liquidity risk* management information, a *firm* should consider other types of information that may be important for understanding its *liquidity risk* profile. This may include:

(1) asset quality and trends;

(2) any changes in the *firm's* funding strategy;

(3) earnings projections; and

(4) the *firm's* reputation in the market and the condition of the market itself.

Limit setting

11.1.30 G A *firm's* senior management should decide what limits need to be set, in accordance with the nature, scale and complexity of its activities. The structure of limits should reflect the need for a *firm* to have systems and controls in place to guard against a spectrum of possible risks, from those arising in day-to-day *liquidity risk* management to those arising in stressed conditions.

11.1.31 G A *firm* should periodically review and, where appropriate, adjust its limits when conditions or risk tolerances change.

11.1.32 G Policy or limit exceptions should receive the prompt attention of the appropriate management and should be resolved according to processes described in approved policies.

Annex D

Senior Management Arrangements, Systems and Controls Handbook (SYSC)

In this Annex, the place where the text is being inserted is indicated and the text is not underlined.

12 Group risk systems and controls requirement

12.1 Application

12.1.1 R Subject to *SYSC* 12.1.2R to *SYSC* 12.1.4R, this section applies to each of the following which is a member of a *group*:

(1) a *firm* that falls into any one or more of the following categories:

(a) a *regulated entity*;

(b) an *ELMI*;

(c) an *insurer*;

(d) a *BIPRU firm*;

(e) a non-*BIPRU firm* that is a *parent financial holding company* in a *Member State* and is a member of a *UK consolidation group*; and

(f) a *firm* subject to the *rules* in *IPRU(INV)* Chapter 14.

(2) a *UCITS firm*, but only if its *group* contains a *firm* falling into (1); and

(3) the *Society*.

12.1.2 R Except as set out in *SYSC* 12.1.4R, this section applies with respect to different types of *group* as follows:

(1) *SYSC* 12.1.8R and *SYSC* 12.1.10R apply with respect to all *groups*, including *FSA regulated EEA financial conglomerates*, other *financial conglomerates* and *groups* dealt with in *SYSC* 12.1.13R to *SYSC* 12.1.16R;

(2) the additional requirements set out in *SYSC* 12.1.11R and *SYSC* 12.1.12R only apply with respect to *FSA regulated EEA financial conglomerates*; and

(3) the additional requirements set out in *SYSC* 12.1.13R to *SYSC* 12.1.16R only apply with respect to *groups* of the kind dealt with by whichever of those *rules* apply.

12.1.3 R This section does not apply to:

(1) an *incoming EEA firm*; or

(2) an *incoming Treaty firm*; or

(3) a *UCITS qualifier*; or

(4) an *ICVC*.

12.1.4 R (1) This *rule* applies in respect of the following *rules*:

(a) *SYSC* 12.1.8R(2);

(b) *SYSC* 12.1.10R(1), so far as it relates to *SYSC* 12.1.8R(2);

(c) *SYSC* 12.1.10R(2); and

(d) *SYSC* 12.1.11R to *SYSC* 12.1.15R.

(2) The *rules* referred to in (1):

(a) only apply with respect to a *financial conglomerate* if it an *FSA regulated EEA financial conglomerate*;

(b) (so far as they apply with respect to a *group* that is not a *financial conglomerate*) do not apply with respect to a *group* for which a *competent authority* in another *EEA state* is lead regulator;

(c) (so far as they apply with respect to a *financial conglomerate*) do not apply to a *firm* with respect to a *financial conglomerate* of which it is a member if the interest of the *financial conglomerate* in that *firm* is no more than a *participation*;

(d) (so far as they apply with respect to other *groups*) do not apply to a *firm* with respect to a *group* of which it is a member if the only relationship of the kind set out in paragraph (3) of the definition of *group* between it and the other members of the *group* is nothing more than a *participation*; and

(e) do not apply with respect to a *third-country group*.

12.1.5 G For the purpose of this section, a *group* is defined in the *Glossary*, and includes the whole of a *firm's* group, including financial and non-financial undertakings. It also covers undertakings with other links to *group* members if their omission from the scope of *group* risk systems and controls would be misleading. The scope of the *group* systems and controls requirements may therefore differ from the scope of the quantitative requirements for *groups*.

Purpose

12.1.6 G The purpose of this chapter is to set out how the systems and control requirements imposed by *SYSC* (Senior Management Arrangements, Systems and Controls) apply where a *firm* is part of a *group*. If a *firm* is a member of a *group*, it should be able to assess the potential impact of risks arising from other parts of its *group* as well as from its own activities.

12.1.7 G This section implements articles 73(3) (Supervision on a consolidated basis of credit institutions) and 138 (Intra-group transactions with mixed activity holding companies) of the *Banking Consolidation Directive*, article 9 of the *Financial Groups Directive* (Internal control mechanisms and risk management processes) and article 8 of the *Insurance Groups Directive* (Intra-group transactions).

General rules

12.1.8 R A *firm* must:

(1) have adequate, sound and appropriate risk management processes and internal control mechanisms for the purpose of assessing and managing its own exposure to *group* risk, including sound administrative and accounting procedures; and

(2) ensure that its *group* has adequate, sound and appropriate risk management processes and internal control mechanisms at the level of the *group*, including sound administrative and accounting procedures.

12.1.9 G For the purposes of *SYSC* 12.1.8R, the question of whether the risk management processes and internal control mechanisms are adequate, sound and appropriate should be judged in the light of the nature, scale and complexity of the *group's* business.

12.1.10 R The internal control mechanisms referred to in *SYSC* 12.1.8R must include:

(1) mechanisms that are adequate for the purpose of producing any data and information which would be relevant for the purpose of monitoring compliance with any prudential requirements (including any reporting requirements and any requirements relating to capital adequacy, solvency, systems and controls and large exposures):

(a) to which the *firm* is subject with respect to its membership of a *group*; or

(b) that apply to or with respect to that *group* or part of it; and

(2) mechanisms that are adequate to monitor funding within the *group*.

Financial conglomerates

12.1.11 R Where this section applies with respect to a *financial conglomerate*, the risk management processes referred to in *SYSC* 12.1.8R(2) must include:

(1) sound governance and management processes, which must include the approval and periodic review by the appropriate managing bodies within the *financial conglomerate* of the strategies and policies of the *financial conglomerate* in respect of all the risks assumed by the *financial conglomerate*, such review and approval being carried out at the level of the *financial conglomerate*;

(2) adequate capital adequacy policies at the level of the *financial conglomerate*, one of the purposes of which must be to anticipate the impact of the business strategy of the *financial conglomerate* on its risk profile and on the capital adequacy requirements to which it and its members are subject;

(3) adequate procedures for the purpose of ensuring that the risk monitoring systems of the *financial conglomerate* and its members are well integrated into their organisation; and

(4) adequate procedures for the purpose of ensuring that the systems and controls of the members of the *financial conglomerate* are consistent and that the risks can be measured, monitored and controlled at the level of the *financial conglomerate*.

12.1.12 R Where this section applies with respect to a *financial conglomerate*, the internal control mechanisms referred to in *SYSC* 12.1.8R(2) must include:

(1) mechanisms that are adequate to identify and measure all material risks incurred by members of the *financial conglomerate* and appropriately relate capital in the *financial conglomerate* to risks; and

(2) sound reporting and accounting procedures for the purpose of identifying, measuring, monitoring and controlling *intra-group transactions and risk concentrations*.

BIPRU firms and other firms to which BIPRU 8 applies

12.1.13 R If this *rule* applies under *SYSC* 12.1.14R to a *firm*, the *firm* must:

(1) comply with *SYSC* 12.1.8R(2) in relation to any *UK consolidation group* or *non-EEA sub-group* of which it is a member, as well as in relation to its *group*; and

(2) ensure that the risk management processes and internal control mechanisms at the level of any *UK consolidation group* or *non-EEA*

sub-group of which it is a member comply with the obligations set out in the following provisions on a consolidated (or sub-consolidated) basis:

(a) *SYSC* 3.2.23R and *SYSC* 3.2.24R;

(b) *SYSC* 3.2.26R;

(c) *SYSC* 3.2.28R to *SYSC* 3.2.36R;

(d) *SYSC* 11.1.11R and *SYSC* 11.1.12R;

(e) *BIPRU* 2.3.7R(1);

(f) *BIPRU* 9.1.6R and *BIPRU* 9.13.21R (Liquidity plans);

(g) *BIPRU* 10.12.3R (Concentration risk policies).

[Note**:** article 73(3) of the *Banking Consolidation Directive*]

12.1.14 R *SYSC* 12.1.13R applies to a *firm* that is:

(1) an *ELMI*;

(2) a *BIPRU firm*; or

(3) a non-*BIPRU firm* that is a *parent financial holding company* in a *Member State* and is a member of a *UK consolidation group*.

12.1.15 R In the case of a *firm* that:

(1) is an *ELMI* or a *BIPRU firm*; and

(2) has a *mixed-activity holding company* as a *parent undertaking*;

the risk management processes and internal control mechanisms referred to in *SYSC* 12.1.8R must include sound reporting and accounting procedures and other mechanisms that are adequate to identify, measure, monitor and control transactions between the *firm's parent undertaking mixed-activity holding company* and any of the *mixed-activity holding company's subsidiary undertakings*.

Insurance undertakings

12.1.16 R In the case of an *insurer* that has a *mixed-activity insurance holding company* as a *parent undertaking*, the risk management processes and internal control mechanisms referred to in *SYSC* 12.1.8R must include sound reporting and accounting procedures and other mechanisms that are adequate to identify, measure, monitor and control transactions between the *firm's parent undertaking mixed-activity insurance holding company* and any of the *mixed-activity insurance holding company's subsidiary undertakings*.

12.1.17 G *SYSC* 12.1.16R cannot apply to a *building society* as it cannot have a *mixed-*

activity holding company as a *parent undertaking*. *SYSC* 12.1.16R cannot apply to a *friendly society* as it cannot have a *mixed-activity insurance holding company* as a *parent undertaking*.

Nature and extent of requirements and allocation of responsibilities within the group

12.1.18 G Assessment of the adequacy of a *group's* systems and controls required by this section will form part of the *FSA's* risk management process.

12.1.19 G The nature and extent of the systems and controls necessary under *SYSC* 12.1.8R(1) to address *group* risk will vary according to the materiality of those risks to the *firm* and the position of the *firm* within the *group*.

12.1.20 G In some cases the management of the systems and controls used to address the risks described in *SYSC* 12.1.8R(1) may be organised on a *group*-wide basis. If the *firm* is not carrying out those functions itself, it should delegate them to the *group* members that are carrying them out. However, this does not relieve the *firm* of responsibility for complying with its obligations under *SYSC* 12.1.8R(1). A *firm* cannot absolve itself of such a responsibility by claiming that any breach of that *rule* is caused by the actions of another member of the *group* to whom the *firm* has delegated tasks. The risk management arrangements are still those of the *firm*, even though personnel elsewhere in the *firm's group* are carrying out these functions on its behalf.

12.1.21 G *SYSC* 12.1.8R(1) deals with the systems and controls that a *firm* should have in respect of the exposure it has to the rest of the *group*. On the other hand, the purpose of *SYSC* 12.1.8R(2) and the *rules* in this section that amplify it is to require *groups* to have adequate systems and controls. However a *group* is not a single legal entity on which obligations can be imposed. Therefore the obligations have to be placed on individual *firms*. The purpose of imposing the obligations on each *firm* in the *group* is to make sure that the *FSA* can take supervisory action against any *firm* in a *group* whose systems and controls do not meet the standards in this section. Thus responsibility for compliance with the *rules* for *group* systems and controls is a joint one.

12.1.22 G If both a *firm* and its *parent undertaking* are subject to *SYSC* 12.1.8R(2), the *FSA* would not expect systems and controls to be duplicated. In this case, the *firm* should assess whether and to what extent it can rely on its parent's *group* risk systems and controls.

Annex E

Senior Management Arrangements, Systems and Controls Handbook (SYSC)

In this Annex, the place where the text is being inserted is indicated and the text is not underlined.

To be inserted after SYSC 12

13 Operational risk: systems and controls

13.1 Application

13.1.1 G *SYSC* 13 applies to an *insurer* unless it is:

(1) a *non-directive friendly society*; or

(2) an *incoming EEA firm*; or

(3) an *incoming Treaty firm*.

13.1.2 G *SYSC* 13 applies to:

(1) an *EEA-deposit insurer*; and

(2) a *Swiss general insurer*;

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*.

13.2 Purpose

13.2.1 G *SYSC* 13 provides *guidance* on how to interpret *SYSC* 3.1.1R and *SYSC* 3.2.6R, 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 Operational risk can affect, amongst other things, a *firm's* solvency, or 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.

13.3 Other related Handbook sections

13.3.1 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) *SYSC* 14 and *INSPRU* 5.1 contain specific *rules* and *guidance* for the establishment and maintenance of operational risk systems and controls in a *prudential context*.

(2) *COB* contains *rules* and *guidance* that can relate to the management of operational risk; for example, *COB* 2 (Rules which apply to all firms conducting designated investment business), *COB* 3 (Financial promotion), *COB* 5 (Advising and selling), *COB* 7 (Dealing and managing) and *COB* 9 (Client assets).

13.4 Requirements to notify the FSA

13.4.1 G Under *Principle* 11 and *SUP* 15.3.1R, a *firm* must notify the *FSA* immediately of any operational risk matter of which the *FSA* would reasonably expect notice. *SUP* 15.3.8G 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 *FSA* 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* 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* 3.2.2G to *SYSC* 3.2.5G for *guidance* on reporting lines and delegation of functions within a *firm* and *SYSC* 3.2.13G to *SYSC* 3.2.14G for *guidance* on the suitability of *employees* and *appointed representatives*. 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 *employee*s. 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* 3.2.18G). 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.

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* 3.2.5G);

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

(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* 13.6.3G 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* 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 (such as *COB* 3 (Financial promotion));

(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 *FSA* 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* 3.2.19G 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* 3.1.1R applies at all times, including when a business continuity plan is invoked. However, the *FSA* 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 *FSA*, *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;

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

13.9 Outsourcing

13.9.1 G As *SYSC* 3.2.4G 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* 15.3.8G(1)(e) explains, a *firm* should notify the *FSA* 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 *FSA* (see *SUP* 2.3.5R (Access to premises) and *SUP* 2.3.7R (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.

13.10 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).

14 Prudential risk management and associated systems and controls

14.1 Application

14.1.1 R This section applies to an *insurer* unless it is:

(1) a *non-directive friendly society*; or

(2) an *incoming EEA firm*; or

(3) an *incoming Treaty firm*.

14.1.2 R This section applies to:

(1) an *EEA-deposit insurer*; and

(2) a *Swiss general insurer*;

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

Purpose

14.1.3 G This section sets out some *rules* and *guidance* on the establishment and maintenance of systems and controls for the management of a *firm's* prudential risks. A *firm's* prudential risks are those that can reduce the adequacy of its financial resources, and as a result may adversely affect confidence in the financial system or prejudice *consumers*. Some key prudential risks are credit, market, liquidity, operational, insurance and group risk.

14.1.4 G The purpose of this section is to serve the *FSA's regulatory objectives* of consumer protection and market confidence. In particular, this section aims to reduce the risk that a *firm* may pose a threat to these *regulatory objectives*, either because it is not prudently managed, or because it has inadequate systems to permit appropriate senior management oversight and control of its business.

14.1.5 G Both adequate financial resources and adequate systems and controls are necessary for the effective management of prudential risks. A *firm* may hold financial resources to help alleviate the financial consequences of minor weaknesses in its systems and controls (to reflect possible impairments in the accuracy or timing of its identification, measurement, monitoring and control of certain risks, for example). However, financial resources cannot adequately compensate for significant weaknesses in a *firm's* systems and controls that could fundamentally undermine its ability to control its affairs effectively.

How to interpret this section

14.1.6 G This section is designed to amplify *Principle* 3 (Management and control) which requires that a *firm* take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems. This section is also designed to be complementary to *SYSC* 2, *SYSC* 3 and *SYSC* 13 in that it contains some additional *rules* and *guidance* on senior management arrangements and associated systems and controls for *firms* that could have a significant impact on the *FSA's* objectives in a *prudential context*.

14.1.7 G In addition to supporting *PRIN* and *SYSC* 2, *SYSC* 3 and *SYSC* 13, this section lays the foundations for the more specific *rules* and *guidance* on the management of credit, market, liquidity, operational, insurance and group risks that are in *SYSC* 11, *SYSC* 12, *SYSC* 15, *SYSC* 16 and *INSPRU* 5.1. Many of the elements raised here in general terms are expanded upon in these sections.

14.1.8 G Appropriate systems and controls for the management of prudential risk will vary from *firm* to *firm*. Therefore, most of the material in this section is *guidance*. In interpreting this *guidance*, a *firm* should have regard to its own particular circumstances. Following from *SYSC* 3.1.2 G, this should include considering the nature, scale and complexity of its business, which may be influenced by factors such as:

(1) the diversity of its operations, including geographical diversity;

(2) the volume and size of its transactions; and

(3) the degree of risk associated with each area of its operation.

14.1.9 G The *guidance* contained within this section is not designed to be exhaustive. When establishing and maintaining its systems and controls a *firm* should have regard not only to other parts of the *Handbook*, but also to material that is issued by other industry or regulatory bodies.

The role of systems and controls in a prudential context

14.1.10 G In a *prudential context*, a *firm's* systems and controls should provide its senior management with an adequate means of managing the *firm*. As such, they should be designed and maintained to ensure that senior management is able to make and implement integrated business planning and risk management decisions on the basis of accurate information about the risks that the *firm* faces and the financial resources that it has.

The prudential responsibilities of senior management and the apportionment of those responsibilities

14.1.11 G Ultimate responsibility for the management of prudential risks rests with a *firm's governing body* and relevant *senior managers*, and in particular with those individuals that undertake the *firm's governing functions* and the

apportionment and oversight function. In particular, these responsibilities should include:

(1) overseeing the establishment of an appropriate business plan and risk management strategy;

(2) overseeing the development of appropriate systems for the management of prudential risks;

(3) establishing adequate *internal controls*; and

(4) ensuring that the *firm* maintains adequate financial resources.

The delegation of responsibilities within the firm

14.1.12 G Although authority for the management of a *firm's* prudential risks is likely to be delegated, to some degree, to individuals at all levels of the organisation, overall responsibility for this activity should not be delegated from its *governing body* and relevant *senior managers*.

14.1.13 G Where delegation does occur, a *firm* should ensure that appropriate systems and controls are in place to allow its *governing body* and relevant *senior managers* to participate in and control its prudential risk management activities. The *governing body* and relevant *senior managers* should approve and periodically review these systems and controls to ensure that delegated duties are being performed correctly.

Firms subject to risk management on a group basis

14.1.14 G Some *firms* organise the management of their prudential risks on a stand-alone basis. In some cases, however, the management of a *firm's* prudential risks may be entirely or largely subsumed within a whole *group* or *sub-group* basis.

(1) The latter arrangement may still comply with the *FSA's* prudential policy on systems and controls if the *firm's governing body* formally delegates the functions that are to be carried out in this way to the *persons* or bodies that are to carry them out. Before doing so, however, the *firm's governing body* should have explicitly considered the arrangement and decided that it is appropriate and that it enables the *firm* to meet the *FSA's* prudential policy on systems and controls. The *firm* should notify the *FSA* if the management of its prudential risks is to be carried out in this way.

(2) Where the management of a *firm's* prudential risks is largely, but not entirely, subsumed within a whole *group* or *sub-group* basis, the *firm* should ensure that any prudential issues that are specific to the *firm* are:

(a) identified and adequately covered by those to whom it has delegated certain prudential risk management tasks; or

(b) dealt with by the *firm* itself.

14.1.15 G Any delegation of the management of prudential risks to another part of a *firm's group* does not relieve it of responsibility for complying with the *FSA's* prudential policy on systems and controls. A *firm* cannot absolve itself of such a responsibility by claiming that any breach of the *FSA's* prudential policy on systems and controls is effected by the actions of a third party *firm* to whom the *firm* has delegated tasks. The risk management arrangements are still those of the *firm*, even though personnel elsewhere in the *firm's group* are carrying out these functions on its behalf. Thus any references in *GENPRU*, *INSPRU* or *SYSC* to what a *firm*, its personnel and its management should and should not do still apply, and do not need any adjustment to cover the situation in which risk management functions are carried out on a *group*-wide basis.

14.1.16 G Where it is stated in *GENPRU*, *INSPRU* or *SYSC* that a particular task in relation to a *firm*'s systems and controls should be carried out by a *firm's governing body* this task should not be delegated to another part of its *group*. Furthermore, even where the management of a *firm*'s prudential risks is delegated as described in *SYSC* 14.1.14G, responsibility for its effectiveness and for ensuring that it remains appropriate remains with the *firm's governing body*. The *firm's governing body* should therefore keep any delegation under review to ensure that delegated duties are being performed correctly.

Business planning and risk management

14.1.17 G Business planning and risk management are closely related activities. In particular, the forward-looking assessment of a *firm's* financial resources needs, and of how business plans may affect the risks that it faces, are important elements of prudential risk management. A *firm's* business planning should also involve the creation of specific risk policies which will normally outline a *firm's* strategy and objectives for, as appropriate, the management of its market, credit, liquidity, operational, insurance and group risks and the processes that it intends to adopt to achieve these objectives. *SYSC* 14.1.18R to *SYSC* 14.1.25G set out some *rules* and *guidance* relating to business planning and risk management in a *prudential context* (see also *SYSC* 3.2.17G, which states that a *firm* should plan its business appropriately).

14.1.18 R A *firm* must take reasonable steps to ensure the establishment and maintenance of a business plan and appropriate systems for the management of prudential risk.

14.1.19 R When establishing and maintaining its business plan and prudential risk management systems, a *firm* must document:

(1) an explanation of its overall business strategy, including its business objectives;

(2) a description of, as applicable, its policies towards market, credit (including provisioning), liquidity, operational, insurance and group risk (that is, its risk policies), including its appetite or tolerance for these risks and how it identifies, measures or assesses, monitors and controls these risks;

(3) the systems and controls that it intends to use in order to ensure that its business plan and risk policies are implemented correctly;

(4) a description of how the *firm* accounts for assets and liabilities, including the circumstances under which items are netted, included or excluded from the *firm's* balance sheet and the methods and assumptions for valuation;

(5) appropriate financial *projections* and the results of its stress testing and scenario analysis (see *GENPRU* 1.2 (Adequacy of financial resources); and

(6) details of, and the justification for, the methods and assumptions used in financial *projections* and stress testing and scenario analysis.

14.1.20 G The prudential risk management systems referred to in *SYSC* 14.1.18R and *SYSC* 14.1.19R are the means by which a *firm* is able to:

(1) identify the prudential risks that are inherent in its business plan, operating environment and objectives, and determine its appetite or tolerance for these risks;

(2) measure or assess its prudential risks;

(3) monitor its prudential risks; and

(4) control or mitigate its prudential risks.

INSPRU 4.1.63E is an *evidential provision* relating to *SYSC* 14.1.18R concerning risk management systems in respect of *liquidity risk* arising from substantial exposures in foreign currencies.

14.1.21 G A *firm* should consider the relationship between its business plan, risk policies and the financial resources that it has available (or can readily access), recognising that decisions made in respect of one element may have consequences for the other two.

14.1.22 G A *firm's* business plan and risk management systems should be:

(1) effectively communicated so that all *employees* and contractors understand and adhere to the procedures related to their own responsibilities;

(2) regularly updated and revised, in particular when there is significant new information or when actual practice or performance differs materially from the documented strategy, policy or systems.

14.1.23 G The level of detail in a *firm's* business plan and its approach to the design of its risk management systems should be appropriate to the scale and complexity of its operations, and the nature and degree of risk that it faces.

14.1.24 G A *firm's* business plan and systems documentation should be accessible to the *firm's* management in line with their respective responsibilities and, upon request, to the *FSA*.

14.1.25 G *SYSC* 14.1.19R(5) requires a *firm* to *document* its financial projections and the results of its stress testing and scenario analysis. Such financial projections, stress tests and scenario analysis should be used by a *firm's governing body* and relevant *senior managers* when deciding upon how much risk the *firm* is willing to accept in pursuit of its business objectives and how risk limits should be set. Further *rules* and *guidance* on stress testing and scenario analysis are outlined in *GENPRU* 1.2 (Adequacy of financial resources) and *SYSC* 11 (Liquidity risk systems and controls).

Internal controls: introduction

14.1.26 G *Internal controls* should provide a *firm* with reasonable assurance that it will not be hindered in achieving its objectives, or in the orderly and legitimate conduct of its business, by events that may reasonably be foreseen. More specifically in a *prudential context, internal controls* should be concerned with ensuring that a *firm's* business plan and risk management systems are operating as expected and are being implemented as intended. The following *rule* (*SYSC* 14.1.27R) reflects the importance of *internal controls* in a *prudential context*.

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.

14.1.29 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* 14.1.28G, 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* 3.2.2G);

(2) how the delegation or contracting of functions or activities to *employees*, *appointed representatives* or other third parties (for example *outsourcing*) is to be monitored and controlled (see *SYSC* 3.2.3G to *SYSC* 3.2.4G, *SYSC* 14.1.12G to *SYSC* 14.1.16G and *SYSC* 14.1.33G; 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* 13.6.3G);

(4) the need for adequate segregation of duties (see *SYSC* 3.2.5G and *SYSC* 14.1.30G to *SYSC* 14.1.33G;

(5) the establishment and control of risk management committees (see *SYSC* 14.1.34G to *SYSC* 14.1.37G);

(6) the need for risk assessment and the establishment of a risk assessment function (see *SYSC* 3.2.10G and *SYSC* 14.1.38G to *SYSC* 14.1.41G;

(7) the need for internal audit and the establishment of an internal audit function and audit committee (see *SYSC* 3.2.15G to *SYSC* 3.2.16G and *SYSC* 14.1.42G to *SYSC* 14.1.45G).

Internal controls: segregation of duties

14.1.30 G The effective segregation of duties is an important internal control in the *prudential context*. In particular, it helps to ensure that no one individual is completely free to commit a *firm's* assets or incur liabilities on its behalf. Segregation can also help to ensure that a *firm's governing body* receives objective and accurate information on financial performance, the risks faced by the *firm* and the adequacy of its systems. In this regard, a *firm* should ensure that there is adequate segregation of duties between *employees* involved in:

(1) taking on or controlling risk (which could involve risk mitigation);

(2) risk assessment (which includes the identification and analysis of risk); and

(3) internal audit.

14.1.31 G In addition, a *firm* should normally ensure that no single individual has

unrestricted authority to do all of the following:

(1) initiate a transaction;

(2) bind the *firm*;

(3) make payments; and

(4) account for it.

14.1.32 G Where a *firm* is unable to ensure the complete segregation of duties (for example, because it has a limited number of staff), it should ensure that there are adequate compensating controls in place (for example, frequent review of an area by relevant *senior managers*).

14.1.33 G Where a *firm* outsources a *controlled function*, such as *internal audit*, it should take reasonable steps to ensure that every individual involved in the performance of this service is independent from the individuals who perform its external audit. This should not prevent services from being undertaken by a *firm's* external auditors provided that:

(1) the work is carried out under the supervision and management of the *firm's* own internal staff; and

(2) potential conflicts of interest between the provision of external audit services and the provision of *controlled functions* are properly managed.

Internal controls: risk management committees

14.1.34 G In many *firms*, especially if there are multiple business lines, it is common for the *governing body* to delegate some tasks related to risk control and management to committees such as asset and liability committees (ALCO), credit risk committees and market risk committees.

14.1.35 G Where a *firm* decides to create one or more risk management committee(s), adequate *internal controls* should be put in place to ensure that these committees are effective and that their actions are consistent with the objectives outlined in *SYSC* 14.1.28G. This should normally include consideration of the following:

(1) setting clear terms of reference, including membership, reporting lines and responsibilities of each committee;

(2) setting limits on their authority;

(3) agreeing routine reporting and non-routine reporting escalation procedures;

(4) agreeing the minimum frequency of committee meetings; and

(5) reviewing the performance of these risk management committees.

14.1.36 G The decision to delegate risk management tasks, along with the terms of reference of the committees and their performance, should be reviewed periodically by the *firm's governing body* and revised as appropriate.

14.1.37 G The effective use of risk management committees can help to enhance a *firm's internal controls*. In establishing and maintaining its risk management committees, a *firm* should consider:

(1) their membership, which should normally include relevant *senior managers* (such as the head of group risk, head of legal, and the heads of market, credit, liquidity and operational risk, etc.), business line managers, risk management personnel and other appropriately skilled people, for example, actuaries, lawyers, accountants, IT specialists, etc.;

(2) using these committees to:

(i) inform the decisions made by a *firm's governing body* regarding its appetite or tolerance for risk taking;

(ii) highlight risk management issues that may require attention by the *governing body*;

(iii) consider risk at the firm-wide level and, within delegated limits, to determine the allocation of risk limits and financial resources across business lines; and

(iv) consider how exposures may be unwound, hedged, or otherwise mitigated, as appropriate.

Internal controls: risk assessment

14.1.38 G Risk assessment is the process through which a *firm* identifies and analyses (using both qualitative and quantitative methodologies) the risks that it faces. A *firm's* risk assessment activities should normally include consideration of:

(1) its total exposure to risk at the *firm*-wide level (that is, its exposure across business lines and risk categories);

(2) capital allocation and the need to calculate risk weighted returns for different business lines;

(3) the potential correlations that can exist between the risks in different business lines; this should also include looking for risks to which a *firm's* business plan is particularly sensitive, such as interest rate risk, or multiple dealings with the same *counterparty*;

(4) the use of stress tests and scenario analysis;

(5) whether there are risks inherent in the *firm's* business that are not being addressed adequately;

(6) the risk adjusted return that the *firm* is achieving; and

(7) the adequacy and timeliness of management information on market, credit, insurance, liquidity, operational and group risks from the business lines, including risk limit utilisation.

14.1.39 G In accordance with *SYSC* 3.2.10G a *firm* should consider whether it needs to set up a separate *risk assessment function* (or functions) that is responsible for assessing the risks that the *firm* faces and advising its *governing body* and *senior managers* on them.

14.1.40 G Where a *firm* does decide that it needs a separate *risk assessment function*, the *employees* or contractors that carry out this function should not normally be involved in risk taking activities such as business line management (see *SYSC* 14.1.30G to *SYSC* 14.1.33G on the segregation of duties).

14.1.41 G A summary of the results of the analysis undertaken by a *firm's risk assessment function* (including, where necessary, an explanation of any assumptions that were adopted) should normally be reported to relevant *senior managers* as well as to the *firm's governing body*.

Internal audit

14.1.42 G A *firm* should ensure that it has appropriate mechanisms in place to assess and monitor the appropriateness and effectiveness of its systems and controls. This should normally include consideration of:

(1) adherence to and effectiveness of, as appropriate, its market, credit, liquidity, operational, insurance, and group risk policies;

(2) whether departures and variances from its documented systems and controls and risk policies have been adequately documented and appropriately reported, including whether appropriate pre-clearance authorisation has been sought for material departures and variances;

(3) adherence to and effectiveness of its accounting policies, and whether accounting records are complete and accurate;

(4) adherence to and effectiveness of its management reporting arrangements, including the timeliness of reporting, and whether information is comprehensive and accurate; and

(5) adherence to *FSA rules* and regulatory prudential standards.

14.1.43 G In accordance with *SYSC* 3.2.15G and *SYSC* 3.2.16G, a *firm* should consider whether it needs to set up a dedicated *internal audit function*.

14.1.44 G Where a *firm* decides to set up an *internal audit function*, this function should provide independent assurance to its *governing body*, audit

committee or an appropriate *senior manager* of the integrity and effectiveness of its systems and controls.

14.1.45 G In forming its judgements, the *person* performing the *internal audit function* should test the practical operation of a *firm's* systems and controls as well as its accounting and risk policies. This should include examining the adequacy of supporting records.

Management information

14.1.46 G Many individuals, at various levels of a *firm*, need management information relating to their activities. However, *SYSC* 14.1.47G to *SYSC* 14.1.50G concentrates on the management information that should be available to those at the highest level of a *firm*, that is, the *firm's governing body* and relevant *senior managers*. In so doing *SYSC* 14.1.47G to *SYSC* 14.1.50G amplify *SYSC* 3.2.11G and *SYSC* 3.2.12G (which outline the *FSA's* high level policy on senior management information) by providing some additional *guidance* on the management information that should be available in a *prudential context*.

14.1.47 G The role of management information should be to help a *firm's governing body* and *senior managers* to understand risk at a firm-wide level. In so doing, it should help them to:

(1) determine whether a *firm* is prudently managed with adequate financial resources;

(2) make the decisions that fall within their ambit (for example, the high level business plans, strategy and risk tolerances of the *firm*); and

(3) oversee the execution of tasks for which they are responsible.

14.1.48 G A *firm* should consider what information needs to be made available to its *governing body* and *senior managers*. Some possible examples include:

(1) firm-wide information such as the overall profitability and value of a *firm* and its total exposure to risk;

(2) reports from committees to which the *governing body* has delegated risk management tasks, if applicable;

(3) reports from a *firm's internal audit* and *risk assessment functions*, if applicable, including exception reports, where risk limits and policies have been breached or systems circumvented;

(4) financial projections under expected and abnormal (that is, stressed) conditions;

(5) reconciliation of actual profit and loss to previous financial projections and an analysis of any significant variances;

(6) matters which require a decision from the *governing body* or *senior*

managers, for example a significant variation to a business plan, amendments to risk limits, the creation of a new business line, etc;

(7) compliance with *FSA rules* and regulatory prudential standards;

(8) risk weighted returns; and

(9) liquidity and funding requirements.

14.1.49 G The management information that is provided to a *firm's governing body* and *senior managers* should have the following characteristics:

(1) it should be timely, its frequency being determined by factors such as:

(a) the volatility of the business in which the *firm* is engaged (that is, the speed at which its risks can change);

(b) any time constraints on when action needs to be taken; and

(c) the level of risk that the *firm* is exposed to, compared to its available financial resources and tolerance for risk;

(2) it should be reliable, having regard to the fact that it may be necessary to sacrifice a degree of accuracy for timeliness; and

(3) it should be presented in a manner that highlights any relevant issues on which those undertaking *governing functions* should focus particular attention.

14.1.50 G The production of management and other information may require the collation of data from a variety of separate manual and automated systems. In such cases, responsibility for the integrity of the information may be spread amongst a number of operational areas. A *firm* should ensure that it has appropriate processes to validate the integrity of its information.

Record keeping

14.1.51 G *SYSC* 3.2.20R requires a *firm* to take reasonable care to make and retain adequate records. The following policy on record keeping supplements *SYSC* 3.2.20R by providing some additional *rules* and *guidance* on record keeping in a *prudential context*. The purpose of this policy is to:

(1) facilitate the prudential supervision of a *firm* by ensuring that adequate information is available regarding its past/current financial situation and business activities (which includes the design and implementation of systems and controls); and

(2) help the *FSA* to satisfy itself that a *firm* is operating in a prudent manner and is not prejudicing the interests of its *customers* or market confidence.

14.1.52 G In addition to the record keeping requirements in *GENPRU*, *INSPRU* and *SYSC*, a *firm* should remember that it may be obliged, under other applicable laws or regulations, to keep similar or additional records.

14.1.53 R (1) A *firm* must make and regularly update accounting and other records that are sufficient to enable the *firm* to demonstrate to the *FSA*:

(a) that the *firm* is financially sound and has appropriate systems and controls;

(b) the *firm's* financial position and exposure to risk (to a reasonable degree of accuracy); and

(c) the *firm's* compliance with the *rules* in *GENPRU*, *INSPRU* and *SYSC*.

(2) The records in (1) must be retained for a minimum of three years, or longer as appropriate.

14.1.54 G A *firm* should be able to make available the records described in *SYSC* 14.1.53 R within a reasonable timeframe when requested to do so by the *FSA*.

14.1.55 G The *FSA* recognises that not all records are specific to a particular point in time. As such, while it may be appropriate to update some records on a daily or continuous basis, for example expenditure and details of certain transactions, it may not be appropriate to update other records as regularly as this, for example those relating to its business plan and risk policies. A *firm* should decide how regularly it should update particular records.

14.1.56 G A *firm* should decide which records it needs to hold, noting that compliance with *SYSC* 14.1.53R does not require it to hold records on every single aspect of its activities. Some specific *guidance* on the types of records that a *firm* should hold is set out in each of the risk specific sections on systems and controls (see *SYSC* 11, *SYSC* 12, *SYSC* 14.1.65G, *SYSC* 15 to *SYSC* 17 and *INSPRU* 5.1).

14.1.57 G In deciding which records to hold, a *firm* should also take into account that failure to keep adequate records could make it harder for it to satisfy the *FSA* that it is compliant with the *rules* in *GENPRU*, *INSPRU* or *SYSC*, and to defend any enforcement action taken against it.

14.1.58 G A *firm* should keep the records required in *GENPRU*, *INSPRU* and *SYSC* in an appropriate format and language (in terms of format this could include holding them on paper or in electronic or some other form). However, whatever format or language a *firm* chooses, *SYSC* 3.2.20R requires that records be capable of being reproduced on paper and in English (except where they relate to business carried on from an establishment situated in a country where English is not an official language).

14.1.59 G In accordance with *SYSC* 3.2.20R, a *firm* should retain the records that it needs to comply with *SYSC* 14.1.53R for as long as they are relevant for the

purposes for which they were made.

14.1.60 R A *firm* must keep the *records* required in *SYSC* 14.1.53R in the *United Kingdom*, except where:

(1) they relate to business carried on from an establishment in a country or territory that is outside the *United Kingdom*; and

(2) they are kept in that country or territory.

14.1.61 R When a *firm* keeps the records required in *SYSC* 14.1.53R outside the *United Kingdom*, it must periodically send an adequate summary of those records to the *United Kingdom*.

14.1.62 G Where a *firm* outsources the storage of some or all of its records to a third party service provider, it should ensure that these records are readily accessible and can be reproduced within a reasonable time period. The *firm* should also ensure that these records are stored in compliance with the *rules* and *guidance* on record keeping in *GENPRU*, *INSPRU* or *SYSC*. Additional *guidance* on the management of *outsourcing* agreements is provided in *SYSC* 13.

14.1.63 G A *firm* may rely on records that have been produced by a third party (for example, another *group* company or an external agent, such as an outsource service provider). However where the *firm* does so it should ensure that these records are readily accessible and can be reproduced within a reasonable time period. The *firm* should also ensure that these records comply with the *rules* and *guidance* on record keeping in *GENPRU*, *INSPRU* or *SYSC*.

14.1.64 G In accordance with *SYSC* 3.2.21G, a *firm* should have adequate systems and controls for maintaining the security of its records so that they are reasonably safeguarded against loss, unauthorised access, alteration or destruction.

Operational risk

14.1.65 G As well as covering other types of risk, the *rules* and *guidance* set out in this chapter deal with a *firm's* approach to operational risk. In particular:

(1) *SYSC* 14.1.18R requires a *firm* to take reasonable steps to ensure that the risk management systems put in place to identify, assess, monitor and control operational risk are adequate for that purpose;

(2) *SYSC* 14.1.19R(2) requires a *firm* to document its policy for operational risk, including its risk appetite and how it identifies, assesses, monitors and controls that risk; and

(3) *SYSC* 14.1.27R requires a *firm* to take reasonable steps to establish and maintain adequate *internal controls* to enable it to assess and

monitor the effectiveness and implementation of its business plan and prudential risk management systems.

15 Credit risk management systems and controls

15.1 Application

15.1.1 G *SYSC* 15.1 applies to an *insurer* unless it is:

(1) a *non-directive friendly society*; or

(2) an *incoming EEA firm*; or

(3) an *incoming Treaty firm*.

15.1.2 G *SYSC* 15.1 applies to:

(1) an *EEA-deposit insurer*; and

(2) a *Swiss general insurer*;

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

Purpose

15.1.3 G This section provides *guidance* on how to interpret *SYSC* 14 insofar as it relates to the management of credit risk.

15.1.4 G Credit risk is incurred whenever a *firm* is exposed to loss if another party fails to perform its financial obligations to the *firm*, including failing to perform them in a timely manner. It arises from both on and off balance sheet items. For contracts for traded *financial instruments*, for example the purchase and sale of *securities* or *over the counter derivatives*, risks may arise if the *firm's counterparty* does not honour its side of the contract. This constitutes counterparty risk, which can be considered a subset of credit risk. Another risk is issuer risk, which could potentially result in a *firm* losing the full price of a market instrument since default by the issuer could result in the value of its bonds or stocks falling to nil. In insurance *firms*, credit risk can arise from *premium* debtors, where cover under *contracts of insurance* may either commence before premiums become due or continue after their non-payment. Credit risk can also arise if a *reinsurer* fails to fulfil its financial obligation to repay a *firm* upon submission of a *claim*.

15.1.5 G Credit risk concerns the *FSA* in a *prudential context* because inadequate systems and controls for credit risk management can create a threat to the *regulatory objectives* of market confidence and consumer protection by:

(1) the erosion of a *firm's* capital due to excessive credit losses thereby threatening its viability as a going concern;

(2) an inability of a *firm* to meet its own obligations to depositors, *policyholders* or other market *counterparties* due to its capital

erosion.

15.1.6 G Appropriate systems and controls for the management of credit risk will vary with the scale, nature and complexity of the *firm's* activities. Therefore the material in this section is *guidance*. A *firm* should assess the appropriateness of any particular item of *guidance* 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.

Requirements

15.1.7 G High level requirements for prudential systems and controls, including those for credit risk, are set out in *SYSC* 14. In particular:

(1) *SYSC* 14.1.19R(2) requires a *firm* to document its policy for credit risk, including its risk appetite and how it identifies, measures, monitors and controls that risk;

(2) *SYSC* 14.1.19R(2) requires a *firm* to document its provisioning policy. Documentation should describe the systems and controls that it intends to use to ensure that the policy is correctly implemented;

(3) *SYSC* 14.1.18R requires it to establish and maintain risk management systems to identify, measure, monitor and control credit risk (in accordance with its credit risk policy), and to take reasonable steps to ensure that its systems are adequate for that purpose; or

(4) in line with *SYSC* 14.1.11G, the ultimate responsibility for the management of credit risk should rest with a *firm's governing body*. Where delegation of authority occurs the *governing body* and relevant *senior managers* should approve and periodically review systems and controls to ensure that delegated duties are being performed correctly.

Credit risk policy

15.1.8 G *SYSC* 14.1.18R requires a *firm* to establish, maintain and document a business plan and risk policies. They should provide a clear indication of the amount and nature of credit risk that the *firm* wishes to incur. In particular, they should cover for credit risk:

(1) how, with particular reference to its activities, the *firm* defines and measures credit risk;

(2) the *firm's* business aims in incurring credit risk including:

(a) identifying the types and sources of credit risk to which the *firm* wishes to be exposed (and the limits on that exposure) and those to which the *firm* wishes not to be exposed (and how that is to be achieved, for example how exposure is to be avoided or mitigated);

(b) specifying the level of diversification required by the *firm* and the *firm's* tolerance for risk concentrations (and the limits on those exposures and concentrations); and

(c) drawing the distinction between activities where credit risk is taken in order to achieve a return (for example, lending) and activities where credit exposure arises as a consequence of pursuing some other objective (for example, the purchase of a *derivative* in order to mitigate *market risk*);

(3) how credit risk is assessed both when credit is granted or incurred and subsequently, including how the adequacy of any security and other risk mitigation techniques is assessed;

(4) the detailed limit structure for credit risk which should:

(a) address all key risk factors, including intra-*group* exposures and indirect exposures (for example, exposures held by *related* and *subsidiary undertakings*);

(b) be commensurate with the volume and complexity of activity; and

(c) be consistent with the *firm's* business aims, historical performance, and its risk appetite;

(5) procedures for:

(a) approving new or additional exposures to *counterparties*;

(b) approving new products and activities that give rise to credit risk;

(c) regular risk position and performance reporting;

(d) limit exception reporting and approval; and

(e) identifying and dealing with the problem exposures caused by the failure or downgrading of a *counterparty*;

(6) the methods and assumptions used for the stress testing and scenario analysis required by *GENPRU* 1.2 (Adequacy of financial resources), including how these methods and assumptions are selected and tested; and

(7) the allocation of responsibilities for implementing the credit risk policy and for monitoring adherence to, and the effectiveness of, the policy.

Counterparty assessment

15.1.9 G The *firm* should make a suitable assessment of the risk profile of the *counterparty*. The factors to be considered will vary according to both the type of credit and the *counterparty* being considered. This may include:

(1) the purpose of the credit, the duration of the agreement and the source of repayment;

(2) an assessment and continuous monitoring of the credit quality of the *counterparty*;

(3) an assessment of the *claims* payment record where the *counterparty* is a *reinsurer*;

(4) an assessment of the nature and amount of risk attached to the *counterparty* in the context of the industrial sector or geographical region or country in which it operates, as well as the potential impact on the *counterparty* of political, economic and market changes; and

(5) the proposed terms and conditions attached to the granting of credit, including ongoing provision of information by the *counterparty*, covenants attached to the facility as well as the adequacy and enforceability of *collateral*, security and guarantees.

15.1.10 G It is important that sound and legally enforceable documentation is in place for each agreement that gives rise to credit risk as this may be called upon in the event of a default or dispute. A *firm* should therefore consider whether it is appropriate for an independent legal opinion to be sought on documentation used by the *firm*. Documentation should normally be in place before the *firm* enters into a contractual obligation or releases funds.

15.1.11 G Where *premium* payments are made via *brokers* or *intermediaries*, the *firm* should describe how it monitors and controls its exposure to those *brokers* and *intermediaries*. In particular, the policy should identify whether the risk of default by the *broker* or *intermediary* is borne by the *firm* or the *policyholder*.

15.1.12 G Any variation from the usual credit policy should be documented.

15.1.13 G A *firm* involved in loan syndications or consortia should not rely on other parties' assessment of the credit risks involved. It will remain responsible for forming its own judgement on the appropriateness of the credit risk thereby incurred with reference to its stated credit risk policy. Similarly a *firm* remains responsible for assessing the credit risk associated with any insurance or *reinsurance* placed on its behalf by other parties.

15.1.14 G Where a credit scoring approach or other *counterparty* assessment process is used, the *firm* should periodically assess the particular approach taken in the light of past and expected future *counterparty* performance and ensure that any statistical process is adjusted accordingly to ensure that the business

written complies with the *firm's* risk appetite.

15.1.15 G In assessing its contingent exposure to a *counterparty*, the *firm* should identify the amount which would be due from the *counterparty* if the value, index or other factor upon which that amount depends were to change.

Credit risk measurement

15.1.16 G A *firm* should measure its credit risk using a robust and consistent methodology which should be described in its credit risk policy; the appropriate method of measurement will depend upon the nature of the credit product provided. The *firm* should consider whether the measurement methodologies should be backtested and the frequency of such backtesting.

15.1.17 G A *firm* should also be able to measure its credit exposure across its entire portfolio or within particular categories such as exposures to particular industries, economic sectors or geographical areas.

15.1.18 G Where a *firm* is a member of a *group* that is subject to consolidated reporting, the *group* should be able to monitor credit exposures on a consolidated basis. See *SYSC* 12, *INSPRU* 6.1 and *GENPRU* 3.

15.1.19 G A *firm* should have the capability to measure its credit exposure to individual *counterparties* on at least a daily basis.

Risk monitoring

15.1.20 G A *firm* should implement an effective system for monitoring its credit risk which should be described in its credit risk policy.

15.1.21 G A *firm* should have a system of management reporting which provides clear, concise, timely and accurate credit risk reports to relevant functions within the *firm*. The reports could cover exceptions to the *firm's* credit risk policy, non-performing exposures and changes to the level of credit risk within the *firm's* credit portfolio. A *firm* should have procedures for taking appropriate action according to the information within the management reports, such as a review of *counterparty* limits, or of the overall credit policy.

15.1.22 G Individual credit facilities and overall limits should be periodically reviewed in order to check their appropriateness for both the current circumstances of the *counterparty* and the *firm's* current internal and external economic environment. The frequency of review should be appropriate to the nature of the facility.

15.1.23 G A *firm* should utilise appropriate stress testing and scenario analysis of credit exposures to examine the potential effects of economic or industry downturns, market events, changes in interest rates, changes in foreign exchange rates, changes in liquidity conditions and changes in levels of insurance losses where relevant.

Problem exposures

15.1.24 G A *firm* should have systematic processes for the timely identification, management and monitoring of problem exposures. These processes should be described in the credit risk policy.

15.1.25 G A *firm* should have adequate procedures for recovering exposures in arrears or that have had provisions made against them. A *firm* should allocate responsibility, either internally or externally, for its arrears management and recovery.

Provisioning

15.1.26 G *SYSC* 14.1.19R(2) requires a *firm* to document its provisioning policy. A *firm's* provisioning policy can be maintained either as a separate document or as part of its credit risk policy.

15.1.27 G At intervals that are appropriate to the nature, scale and complexity of its activities a *firm* should review and update its provisioning policy and associated systems.

15.1.28 G In line with *SYSC* 15.1.6G, the *FSA* recognises that the frequency with which a *firm* reviews its provisioning policy once it has been established will vary from *firm* to *firm.* However, the *FSA* expects a *firm* to review at least annually whether its policy remains appropriate for the business it undertakes and the economic environment in which it operates.

15.1.29 G In line with *SYSC* 14.1.12G, the provisioning policy referred to in *SYSC* 15.1.26G must be approved by the *firm's governing body* or another appropriate body to which the *firm's governing body* has delegated this responsibility.

15.1.30 G In line with *SYSC* 14.1.24G, the *FSA* may request a *firm* to provide it with a copy of its current provisioning policy.

15.1.31 G Provisions may be general (against the whole of a given portfolio), specific (against particular exposures identified as bad or doubtful) or both. The *FSA* expects contingent liabilities (for example guarantees) and anticipated losses to be recognised in accordance with accepted accounting standards at the relevant time, such as those embodied in the Financial Reporting Standards issued by the Accounting Standards Board.

Risk mitigation

15.1.32 G A *firm* may choose to use various credit risk mitigation techniques including the taking of *collateral*, the use of letters of credit or guarantees, or *counterparty netting* agreements to manage and control their *counterparty* exposures. The use of such techniques does not obviate the need for thorough credit analysis and procedures. The reliance placed by a *firm* on *risk* mitigation should be described in the credit risk policy.

15.1.33 G A *firm* should consider the legal and financial ability of a guarantor to fulfil the guarantee if called upon to do so.

15.1.34 G A *firm* should monitor the validity and enforceability of its *collateral* arrangements.

15.1.35 G The *firm* should analyse carefully the protection afforded by risk mitigants such as netting agreements or credit *derivatives*, to ensure that any residual risk is identified, measured, monitored and controlled.

Record keeping

15.1.36 G Prudential records made under *SYSC* 14.1.53R should include appropriate records of:

(1) credit exposures, including aggregations of credit exposures, as appropriate, by:

(a) groups of connected *counterparties*; or

(b) types of *counterparty* as defined, for example, by the nature or geographical location of the *counterparty*;

(2) credit decisions, including details of the decision and the facts or circumstances upon which it was made; and

(3) information relevant to assessing current *counterparty* and risk quality.

15.1.37 G Credit records should be retained as long as they are needed for the purpose described in *SYSC* 15.1.36G (subject to the minimum three year retention period). In particular, a *firm* should consider whether it is appropriate to retain information regarding *counterparty* history such as a record of credit events as well as a record indicating how credit decisions were taken.

16 Market risk management systems and controls

16.1 Application

16.1.1 G *SYSC* 16.1 applies to an *insurer* unless it is:

(1) a *non-directive friendly society*; or

(2) an *incoming EEA firm*; or

(3) an *incoming Treaty firm*.

16.1.2 G *SYSC* 16.1 applies to:

(1) an *EEA-deposit insurer*; and

(2) a *Swiss general insurer*;

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

16.1.3 G *Firms* should also see *GENPRU* 1.2 (*GENPRU* 1.2.64G to *GENPRU* 1.2.78G) and *INSPRU* 3.1.

Purpose

16.1.4 G (1) The purpose of this section is to amplify *SYSC* 14 insofar as it relates to *market risk*.

(2) *Market risk* includes equity, interest rate, foreign exchange (FX), commodity risk and interest rate risk on *long-term insurance contracts*. The price of *financial instruments* may also be influenced by other risks such as *spread risk*, *basis risk*, correlation, *specific risk* and *volatility risk*.

(3) This section does not deal with the risk management of *market risk* in a *group* context. A *firm* that is a member of a *group* should also read *SYSC* 12 (Group risk systems and controls) which outlines the *FSA's* requirements for the risk management of *market risk* within a *group*.

(4) Appropriate systems and controls for the management of *market risk* will vary with the scale, nature and complexity of the *firm's* activities. Therefore the material in this section is *guidance*. A *firm* should assess the appropriateness of any particular item of *guidance* 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.

Requirements

16.1.5 G High level requirements for prudential systems and controls, including those for *market risk*, are set out in *SYSC* 14. In particular:

(1) *SYSC* 14.1.19R(2) requires a *firm* to document its policy for *market risk*, including its risk appetite and how it identifies, measures, monitors and controls that risk;

(2) *SYSC* 14.1.19R(4) requires a *firm* to document its asset and liability recognition policy. Documentation should describe the systems and controls that it intends to use to comply with the policy;

(3) *SYSC* 14.1.19R requires a *firm* to establish and maintain risk management systems to identify, measure, monitor and control *market risk* (in accordance with its *market risk* policy), and to take reasonable steps to establish systems adequate for that purpose; and

(4) In line with *SYSC* 14.1.11G, the ultimate responsibility for the management of *market risk* should rest with a *firm's governing body*. Where delegation of authority occurs the *governing body* and relevant *senior managers* should approve and adequately review systems and controls to check that delegated duties are being performed correctly.

Market risk policy

16.1.6 G *SYSC* 14 requires a *firm* to establish, maintain and document a business plan and risk policies. They should provide a clear indication of the amount and nature of *market risk* that the *firm* wishes to incur. In particular, they should cover for *market risk*:

(1) how, with particular reference to its activities, the *firm* defines and measures *market risk*;

(2) the *firm's* business aims in incurring *market risk* including:

(a) identifying the types and sources of *market risk* to which the *firm* wishes to be exposed (and the limits on that exposure) and those to which the *firm* wishes not to be exposed (and how that is to be achieved, for example how exposure is to be avoided or mitigated); and

(b) specifying the level of diversification required by the *firm* and the *firm's* tolerance for risk concentrations (and the limits on those exposures and concentrations).

16.1.7 G The *market risk* policy of a *firm* should be endorsed by the *firm's governing body* and implemented by its senior management, who should take adequate steps to disseminate the policy and train the relevant staff such that they can effectively implement the policy.

16.1.8 G The *market risk* policy of a *firm* should enforce the risk management and control principles and include detailed information on:

(1) the *financial instruments*, commodities, assets and liabilities (and mismatches between assets and liabilities) that a *firm* is exposed to and the limits on those exposures;

(2) the *firm's* investment strategy as applicable between each insurance fund;

(3) activities that are intended to hedge or mitigate *market risk* including mismatches caused by for example differences in the assets and liabilities and maturity mismatches; and

(4) the methods and assumptions used for measuring linear, non-linear and geared *market risk* including the rationale for selection, ongoing validation and testing. Methods might include stress testing and scenario analysis, asset/liability analysis, correlation analysis, Value-at-Risk (VaR) and *options* such as delta, gamma, vega, rho and theta. Exposure to non-linear or geared *market risk* is typically through the use of *derivatives*.

Risk identification

16.1.9 G A *firm* should have in place appropriate risk reporting systems that enable it to identify the types and amount of *market risk* to which it is, and potentially could be, exposed. The information that systems should capture may include but is not limited to:

(1) position information which may include a description of individual *financial instruments* and their cash flows; and

(2) market data which may consist of raw time series of market rates, index levels and prices and derived time series of benchmark yield curves, spreads, implied volatilities, historical volatilities and correlations.

Risk measurement

16.1.10 G Having identified the *market risk* that the *firm* is exposed to on at least a daily basis, a *firm* should be able to measure and manage that *market risk* on a consistent basis. This may be achieved by:

(1) regularly stress testing all or parts of the *firm's* portfolio to estimate potential economic losses in a range of market conditions including abnormal markets. Corporate level stress test results should be discussed regularly by risk monitors, senior management and risk takers, and should guide the *firm's market risk* appetite (for example, stress tests may lead to discussions on how best to unwind or hedge a position), and influence the internal capital allocation process;

(2) measuring the *firm's* exposure to particular categories of *market risk* (for example, equity, interest rate, foreign exchange and commodities) as well as across its entire portfolio of *market risks*;

(3) analysing the impact that new transactions or businesses may have on its *market risk* position on an on-going basis; and

(4) regularly backtesting realised results against internal model generated *market risk* measures in order to evaluate and assess its accuracy. For example, a *firm* should keep a database of daily risk measures such as VaR and *options* such as delta, gamma, vega, rho and theta, and use these to back test predicted profit and loss against actual profit and loss for all trading desks and business units, and monitor the number of exceptions from agreed confidence bands.

Valuation

16.1.11 G A *firm* should take reasonable steps to establish systems and control procedures such that the *firm* complies with the requirements of *GENPRU* 1.3 (Valuation).

16.1.12 G The systems and controls referred to in *SYSC* 16.1.11G should include the following:

(1) the department responsible for the validation of the value of assets and liabilities should be independent of the business trading area, and should be adequately resourced by suitably qualified staff. The department should report to a suitably qualified individual, independent from the business trading area, who has sufficient authority to enforce the systems and controls policies and any alterations to valuation treatments where necessary;

(2) all valuations should be checked and validated at appropriate intervals. Where a *firm* has chosen not to validate all valuations on a daily basis this should be agreed by senior management;

(3) a *firm* should establish a review procedure to check that the valuation procedures are followed and are producing valuations in compliance with the requirements in this section. The review should be undertaken by suitably qualified staff independent of the business trading area, on a regular and ad hoc basis. In particular, this review procedure should include:

(a) the quality and appropriateness of the price sources used;

(b) valuation reserves held; and

(c) the valuation methodology employed for each product and consistent adherence to that methodology;

(4) where a valuation is disputed and the dispute cannot be resolved in a timely manner it should be reported to senior management. It should

continue to be reported to senior management until agreement is reached;

(5) where a *firm* is marking positions to market it should take reasonable steps to establish a price source that is reliable and appropriate to enable compliance with the provisions in this section on an ongoing basis;

(6) a *firm* should document its policies and procedures relating to the entire valuation process. In particular, the following should be documented:

(a) the valuation methodologies employed for all product categories;

(b) details of the price sources used for each product;

(c) the procedures to be followed where a valuation is disputed;

(d) the valuation adjustment and reserving policies;

(e) the level at which a difference between a valuation assigned to an asset or liability and the valuation used for validation purposes will be reported on an exceptions basis and investigated;

(f) where a *firm* is using its own internal estimate to produce a valuation, it should document in detail the process followed in order to produce the valuation; and

(g) the review procedures established by a *firm* in relation to the requirements of this section should be adequately documented and include the rationale for the policy;

(7) a *firm* should maintain records which demonstrate:

(a) senior management's approval of the policies and procedures established; and

(b) management sign-off of the reviews undertaken in accordance with *SYSC* 16.1.11G.

Risk monitoring

16.1.13 G Risk monitoring is the operational process by which a *firm* monitors compliance with defined policies and procedures of the *market risk* policy. The *firm's* risk monitoring system should be independent of the *employees* who are responsible for exposing the *firm* to *market risk*.

16.1.14 G The *market risk* policy of a *firm* may require the production of *market risk* reports at various levels within the *firm*. These reports should provide sufficiently accurate *market risk* data to relevant functions within the *firm*,

and should be timely enough to allow any appropriate remedial action to be proposed and taken, for example:

(1) at a *firm* wide level, a *market risk* report may include information:

(a) summarising and commenting on the total *market risk* that a *firm* is exposed to and *market risk* concentrations by business unit, asset class and country;

(b) on VaR reports against risk limits by business unit, asset class and country;

(c) commenting on significant risk concentrations and market developments; and

(d) on *market risk* in particular legal entities and geographical regions;

(2) at the business unit level, a *market risk* report may include information summarising *market risk* by currency, trading desk, maturity or duration band, or by instrument type;

(3) at the trading desk level, a *market risk* report may include detailed information summarising *market risk* by individual trader, instrument, position, currency, or maturity or duration band; and

(4) all risk data should be readily reconcilable back to the prime books of entry with a fully documented audit trail.

16.1.15 G Risk monitoring may also include information on:

(1) the procedures for taking appropriate action in response to the information within the *market risk* reports;

(2) ensuring that there are controls and procedures for identifying and reporting trades and positions booked at off-market rates;

(3) the process for new product approvals;

(4) the process for dealing with situations (authorised and unauthorised) where particular *market risk* exposures exceed predetermined risk limits and criteria; and

(5) the periodic review of the risk monitoring process in order to check its suitability for both current market conditions and the *firm's* overall risk appetite.

16.1.16 G Risk monitoring should be subject to periodic independent review by suitably qualified staff.

Risk control

16.1.17 G Risk control is the independent monitoring, assessment and supervision of business units within the defined policies and procedures of the *market risk* policy. This may be achieved by:

(1) setting an appropriate *market risk* limit structure to control the *firm's* exposure to *market risk*; for example, by setting out a detailed *market risk* limit structure at the corporate level, the business unit level and the trading desk level which addresses all the key *market risk* factors and is commensurate with the volume and complexity of activity that the *firm* undertakes;

(2) setting limits on risks such as price or rate risk, as well as those factors arising from *options* such as delta, gamma, vega, rho and theta;

(3) setting limits on net and gross positions, *market risk* concentrations, the maximum allowable loss (also called "stop-loss"), VaR, potential risks arising from stress testing and scenario analysis, gap analysis, correlation, liquidity and volatility; and

(4) considering whether it is appropriate to set intermediate (early warning) thresholds that alert management when limits are being approached, triggering review and action where appropriate.

Record keeping

16.1.18 G High level requirements for record keeping are set out in *SYSC* 14.

16.1.19 G In relation to *market risk*, a *firm* should retain appropriate prudential records of:

(1) off and on market trades in *financial instruments*;

(2) the nature and amounts of off and on balance sheet exposures, including the aggregation of exposures;

(3) trades in *financial instruments* and other assets and liabilities; and

(4) methods and assumptions used in stress testing and scenario analysis and in VaR models.

16.1.20 G A *firm* should keep a data history to enable it to perform back testing of methods and assumptions used for stress testing and scenario analysis and for VaR models.

17 Insurance risk systems and controls

17.1 Application

17.1.1 G *SYSC* 17.1 applies to an *insurer* unless it is:

(1) a *non-directive friendly society*; or

(2) an *incoming EEA firm;* or

(3) an *incoming Treaty firm*.

17.1.2 G *SYSC* 17.1 applies to:

(1) an *EEA-deposit insurer*; and

(2) a *Swiss general insurer*;

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

Purpose

17.1.3 G This section provides *guidance* on how to interpret *SYSC* 14 (Prudential risk management and associated systems and controls) in so far as it relates to the management of insurance risk. Insurance risk refers to fluctuations in the timing, frequency and severity of insured events, relative to the expectations of the *firm* at the time of underwriting. Insurance risk can also refer to fluctuations in the timing and amount of *claim* settlements. For *general insurance business* some specific examples of insurance risk include variations in the amount or frequency of *claims* or the unexpected occurrence of multiple *claims* arising from a single cause. For *long-term insurance business* examples include variations in the mortality and persistency rates of *policyholders*, or the possibility that guarantees could acquire a value that adversely affects the finances of a *firm* and its ability to treat its *policyholders* fairly consistent with the *firm's* obligations under *Principle* 6. More generally, insurance risk includes the potential for expense overruns relative to pricing or provisioning assumptions.

17.1.4 G Insurance risk concerns the *FSA* in a *prudential context* because inadequate systems and controls for its management can create a threat to the *regulatory objectives* of market confidence and consumer protection. Inadequately managed insurance risk may result in:

(1) the inability of a *firm* to meet its contractual insurance liabilities as they fall due; and

(2) the inability of a *firm* to treat its *policyholders* fairly consistent with the *firm's* obligations under *Principle* 6 (for example, in relation to bonus payments).

17.1.5 G *Guidance* on the application of this section to a *firm* that is a member of a *group* is provided in *SYSC* 12 (Group risk systems and controls).

17.1.6 G The *guidance* contained within this section should be read in conjunction with the rest of *SYSC.*

17.1.7 G Appropriate systems and controls for the management of insurance risk will vary with the scale, nature and complexity of a *firm's* activities. Therefore, the material in this section is *guidance*. A *firm* should assess the appropriateness of any particular item of *guidance* 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.

General requirements

17.1.8 G High level *rules* and *guidance* for prudential systems and controls for insurance risk are set out in *SYSC* 14. In particular:

(1) *SYSC* 14.1.18R requires a *firm* to take reasonable steps to establish and maintain a business plan and appropriate risk management systems;

(2) *SYSC* 14.1.19R(2) requires a *firm* to document its policy for insurance risk, including its risk appetite and how it identifies, measures, monitors and controls that risk; and

(3) *SYSC* 14.1.27R requires a *firm* to take reasonable steps to establish and maintain adequate *internal controls* to enable it to assess and monitor the effectiveness and implementation of its business plan and prudential risk management systems.

Insurance risk policy

17.1.9 G A *firm's* insurance risk policy should outline its objectives in carrying out *insurance business*, its appetite for insurance risk and its policies for identifying, measuring, monitoring and controlling insurance risk. The insurance risk policy should cover any activities that are associated with the creation or management of insurance risk. For example, underwriting, *claims* management and settlement, assessing *technical provisions* in the balance sheet, risk mitigation and risk transfer, record keeping and management reporting. Specific matters that should normally be in a *firm's* insurance risk policy include:

(1) a statement of the *firm's* willingness and capacity to accept insurance risk;

(2) the classes and characteristics of *insurance business* that the *firm* is prepared to accept;

(3) the underwriting criteria that the *firm* intends to adopt, including how these can influence its rating and pricing decisions;

(4) its approach to limiting significant aggregations of insurance risk, for example, by setting limits on the amount of business that can be underwritten in one region or with one *policyholder*;

(5) where relevant, the *firm's* approach to pricing *long-term insurance contracts*, including the determination of the appropriate level of any reviewable *premiums*;

(6) the *firm's* policy for identifying, monitoring and managing risk when it has delegated underwriting authority to another party (additional *guidance* on the management of *outsourcing* arrangements is provided in *SYSC* 13.9);

(7) the *firm's* approach to managing its expense levels, including acquisition costs, recurring costs, and one-off costs, taking account of the margins available in both the prices for products and in the *technical provisions* in the balance sheet;

(8) the *firm's* approach to the exercise of any discretion (e.g. on charges or the level of benefits payable) that is available in its *long-term insurance contracts*, in the context also of the legal and regulatory constraints existing on the application of this discretion;

(9) the *firm's* approach to the inclusion of options within new *long-term insurance contracts* and to the possible exercise by *policyholders* of options on existing contracts;

(10) the *firm's* approach to managing persistency risk;

(11) the *firm's* approach to managing risks arising from timing differences in taxation or from changes in tax laws;

(12) the *firm's* approach to the use of *reinsurance* or the use of some other means of risk transfer;

(13) how the *firm* intends to assess the effectiveness of its risk transfer arrangements and manage the residual or transformed risks (for example, how it intends to handle disputes over contract wordings, potential payout delays and *counterparty* performance risks);

(14) a summary of the data and information to be collected and reported on underwriting, *claims* and risk control (including internal accounting records), management reporting requirements and external data for risk assessment purposes;

(15) the risk measurement and analysis techniques to be used for setting underwriting *premiums, technical p*rovisions in the balance sheet, and assessing capital requirements; and

(16) the *firm's* approach to stress testing and scenario analysis, as required by *GENPRU* 1.2 (Adequacy of financial resources), including the methods adopted, any assumptions made and the use that is to be

made of the results.

17.1.10 G Further, more detailed, *guidance* is given in *SYSC* 17.1.11G to *SYSC* 17.1.37G on the identification, measurement, monitoring and control (including the use of *reinsurance* and other forms of risk transfer) of insurance risk. A *firm* should consider what additional material to that set out above should be included in its insurance risk policy on each of these for its various activities.

Risk identification

17.1.11 G A *firm* should seek to identify the causes of fluctuations in the occurrence, amount and timing of its insurance liabilities. A *firm* should also seek to identify aggregations of risk that may give rise to large single or multiple *claims*.

17.1.12 G The identification of insurance risk should normally include:

(1) in connection with the *firm's* business plan:

(a) processes for identifying the types of insurance risks that may be associated with a new product and for comparing the risk types that are present in different classes of business (in order to identify possible aggregations in particular insurance risks); and

(b) processes for identifying business environment changes (for example landmark legal rulings) and for collecting internal and external data to test and modify business plans;

(2) at the point of sale, processes for identifying the underwriting risks associated with a particular *policyholder* or a group of *policyholders* (for example, processes for identifying potential *claims* for mis-selling and for collecting information on the *claims* histories of *policyholders*, including whether they have made any potentially false or inaccurate claims, to identify possible adverse selection or moral hazard problems);

(3) after the point of sale, processes for identifying potential and emerging *claims* for the purposes of *claims* management and *claims* provisioning; this could include:

(a) identifying possible judicial rulings;

(b) keeping up to date with developments in market practice; and

(c) collecting information on industry wide initiatives and settlements.

17.1.13 G A *firm* should also identify potential pricing risks, where the liabilities or costs arising from the sale of a product may not be as expected.

Risk measurement

17.1.14 G A *firm* should have in place appropriate systems for collecting the data it needs to measure insurance risk. At a minimum this data should be capable of allowing a *firm* to evaluate the types of *claims* experienced, *claims* frequency and severity, expense levels, persistency levels and, where relevant, potential changes in the value of guarantees and options in *long-term insurance contracts*.

17.1.15 G A *firm* should ensure that the data it collects and the measurement methodologies that it uses are sufficient to enable it to evaluate, as appropriate:

(1) its exposure to insurance risk at all relevant levels, for example, by contract, *policyholder*, product line or insurance class;

(2) its exposure to insurance risk across different geographical areas and time horizons;

(3) its total, *firm*-wide, exposure to insurance risk and any other risks that may arise out of the *contracts of insurance* that it issues;

(4) how changes in the volume of business (for example via changes in *premium* levels or the number of new contracts that are underwritten) may influence its exposure to insurance risk;

(5) how changes in *policy* terms may influence its exposure to insurance risk; and

(6) the effects of specific loss scenarios on the insurance liabilities of the *firm*.

17.1.16 G A *firm* should hold data in a manner that allows for it to be used in a flexible way. For example, data should be sufficiently detailed and disaggregated so that contract details may be aggregated in different combinations to assess different risks.

17.1.17 G A *firm* should be able to justify its choice of measurement methodologies. This justification should normally be documented.

17.1.18 G A *firm* should periodically review the appropriateness of the measurement methodologies that it uses. This could, for example, include back testing (that is, by comparing actual versus expected results) and updating for changes in market practice.

17.1.19 G A *firm* should ensure that it has access to the necessary skills and resources that it needs to measure insurance risk using its chosen methodology.

17.1.20 G When measuring its insurance risks, a *firm* should consider how emerging experience could be used to update its underwriting process, in particular in relation to contract terms and pricing and also its assessment of the *technical*

provisions in the balance sheet.

17.1.21 G A *firm* should have the capability to measure its exposure to insurance risk on a regular basis. In deciding on the frequency of measurement, a *firm* should consider:

(1) the time it takes to acquire and process all necessary data;

(2) the speed at which exposures could change; and

(3) that it may need to measure its exposure to certain types of insurance risk on a daily basis (for example, weather catastrophes).

Risk monitoring

17.1.22 G A *firm* should provide regular and timely information on its insurance risks to the appropriate level of management. This could include providing reports on the following:

(1) a statement of the *firm's* profits or losses for each class of business that it underwrites (with an associated analysis of how these have arisen for any *long-term insurance contracts*), including a variance analysis detailing any deviations from budget or changes in the key performance indicators that are used to assess the success of its business plan for insurance;

(2) the *firm's* exposure to insurance risk at all relevant levels (see *SYSC* 17.1.15G(1)), as well as across different geographical areas and time zones (see *SYSC* 17.1.15G(2)), also senior management should be kept informed of the *firm's* total exposure to insurance risk (see *SYSC* 17.1.15G(3));

(3) an analysis of any internal or external trends that could influence the *firm's* exposure to insurance risk in the future (e.g. new weather patterns, socio-demographic changes, expense overruns etc);

(4) any new or emerging developments in *claims* experience (e.g. changes in the type of *claims*, average *claim* amounts or the number of similar *claims*);

(5) the results of any stress testing or scenario analyses;

(6) the amount and details of new business written and the amount of business that has lapsed or been cancelled;

(7) identified fraudulent *claims*;

(8) a watch list, detailing, for example, material/catastrophic events that could give rise to significant numbers of new *claims* or very large *claims*, contested *claims*, client complaints, legal and other developments;

(9) the performance of any *reinsurance*/risk transfer arrangements; and

(10) progress reports on matters that have previously been referred under escalation procedures (see *SYSC* 17.1.23G).

17.1.23 G A *firm* should establish and maintain procedures for the escalation of appropriate matters to the relevant level of management. Such matters may include:

(1) any significant new exposures to insurance risk, including for example any landmark rulings in the courts;

(2) a significant increase in the size or number of *claims*;

(3) any breaches of the limits set out in *SYSC* 17.1.27G and *SYSC* 17.1.28G, in particular senior management should be informed where any maximum limits have been breached (see *SYSC* 17.1.29G); and

(4) any unauthorised deviations from its insurance risk policy (including those by a *broker*, *appointed representative* or other delegated authority).

17.1.24 G A *firm* should regularly monitor the effectiveness of its analysis techniques for setting provisions for *claims* on *general insurance contracts*.

17.1.25 G A *firm* should have appropriate procedures in place to allow managers to monitor the application (and hence the effect) of its *reinsurance* programme. This would include, for a general *insurer*, procedures for monitoring how its *reinsurance* programme affects the gross provisions that it makes for outstanding *claims* (including *claims* that are incurred but not reported).

Risk control

17.1.26 G A *firm* should take appropriate action to ensure that it is not exposed to insurance risk in excess of its risk appetite. In so doing, the *firm* should be both reactive, responding to actual increases in exposure, and proactive, responding to potential future increases. Being proactive should involve close co-ordination between the processes of risk control, risk identification and risk measurement, as potential future exposures need to be identified and understood before effective action can be taken to control them.

17.1.27 G A *firm* should consider setting limits for its exposure to insurance risk, which trigger action to be taken to control exposure. Periodically these limits should be amended in the light of new information (e.g. on the expected number or size of *claims*). For example, limits could be set for:

(1) the *firm's* aggregate exposure to a single source of insurance risk or for events that may be the result of a number of different sources;

(2) the *firm's* exposure to specific geographic areas or any other groupings of risks whose outcomes may be positively correlated;

(3) the number of fraudulent *claims*;

(4) the number of very large *claims* that could arise;

(5) the number of unauthorised deviations from its insurance risk policy;

(6) the amount of insurance risk than can be transferred to a particular *reinsurer*;

(7) the level of expenses incurred in respect of each relevant business area; and

(8) the level of persistency by product line or distribution channel.

17.1.28 G A *firm* should also consider setting individual underwriting limits for all *employees* and agents that have the authority to underwrite insurance risk. This could include both monetary limits and limits on the types of risk that they can underwrite. Where individual underwriting limits are set, the *firm* should ensure that they are adhered to.

17.1.29 G In addition to setting some 'normal' limits for insurance risk, a *firm* should consider setting some maximum limits, beyond which immediate, emergency action should be taken. These maximum limits could be determined through stress testing and scenario analysis.

17.1.30 G A *firm* should pay close attention to the wording of its *policy* documentation to ensure that these wordings do not expose it to more, or higher, *claims* than it is expecting. In so doing, the *firm* should consider:

(1) whether it has adequate in-house legal resources;

(2) the need for periodic independent legal review of *policy* documentation;

(3) the use of standardised documentation and referral procedures for variation of terms;

(4) reviewing the documentation used by other insurance companies;

(5) revising documentation for new *policies* in the light of past experience; and

(6) the operation of law in the jurisdiction of the *policyholder*.

17.1.31 G A *firm* should ensure that it has appropriate systems and controls for assessing the validity of *claims*. This could involve consideration of the evidence that will be required from *policyholders* and how this evidence is to be tested as well as procedures to determine when experts such as loss

adjusters, lawyers or accountants should be used.

17.1.32 G Particular care should be taken to ensure that a *firm* has appropriate systems and controls to deal with large *claims* or large groups of *claims* that could significantly deplete its financial resources. This should include systems to ensure that senior management (that is, the *governing body* and relevant *senior managers*) is involved in the processing of such *claims* from the outset.

17.1.33 G A *firm* should consider how it intends to use *reinsurance* or some other form of insurance risk transfer agreement to help to control its exposure to insurance risk. Additional *guidance* on the use of *reinsurance*/risk transfer is provided below.

Reinsurance and other forms of risk transfer

17.1.34 G Before entering into or significantly changing a *reinsurance* agreement, or any other form of insurance risk transfer agreement, a *firm* should:

(1) analyse how the proposed *reinsurance*/risk transfer agreement will affect its exposure to insurance risk, its underwriting strategy and its ability to meet its regulatory obligations;

(2) ensure there are adequate legal checking procedures in respect of the draft agreement;

(3) conduct an appropriate due diligence of the *reinsurer's* financial stability (that is, solvency) and expertise; and

(4) understand the nature and limits of the agreement (particular attention should be given to the wording of contracts to ensure that all of the required risks are covered, that the level of available cover is appropriate, and that all the terms, conditions and warranties are unambiguous and understood).

17.1.35 G In managing its *reinsurance* agreements, or any other form of insurance risk transfer agreement, a *firm* should have in place appropriate systems that allow it to maintain its desired level of cover. This could involve systems for:

(1) monitoring the risks that are covered (that is, the scope of cover) by these agreements and the level of available cover;

(2) keeping underwriting staff informed of any changes in the scope or level of cover;

(3) properly co-ordinating all *reinsurance*/risk transfer activities so that, in aggregate, the desired level and scope of cover is maintained;

(4) ensuring that the *firm* does not become overly reliant on any one *reinsurer* or other risk transfer provider; or

(5) conducting regular stress testing and scenario analysis to assess the resilience of its *reinsurance* and risk transfer programmes to catastrophic events that may give rise to large and or numerous *claims*.

17.1.36 G In making a claim on a *reinsurance* contract (that is, its *reinsurance* recoveries) or some other risk transfer contract a *firm* should ensure:

(1) that it is able to identify and recover any money that it is due in a timely manner; and

(2) that it makes adequate financial provision for the risk that it is unable to recover any money that it expected to be due, as a result of either a dispute with or a default by the *reinsurer*/risk transfer provider. Additional *guidance* on credit risk in *reinsurance*/risk transfer contracts is provided in *INSPRU* 2.1 (Credit risk in insurance)].

17.1.37 G Where the planned level or scope of cover from a *reinsurance*/risk transfer contract is not obtained, a *firm* should consider revising its underwriting strategy.

Record keeping

17.1.38 G The *FSA's* high level *rules* and *guidance* for record keeping are outlined in *SYSC* 3.2.20R (Records). Additional *rules* and *guidance* in relation to the *prudential context* are set out in *SYSC* 14.1.51G to *SYSC* 14.1.64G. In complying with these *rules* and *guidance*, a *firm* should retain an appropriate record of its insurance risk management activities. This may, for example, include records of:

(1) each new risk that is underwritten (noting that these records may be held by agents or cedants, rather than directly by the *firm* provided that the *firm* has adequate access to those records);

(2) any material aggregation of exposure to risk from a single source, or of the same kind or to the same potential catastrophe or event;

(3) each notified *claim* including the amounts notified and paid, precautionary notices and any re-opened *claims*;

(4) *policy* and contractual documents and any relevant representations made to *policyholders*;

(5) other events or circumstances relevant to determining the risks and commitments that arise out of *contracts of insurance* (including discretionary benefits and charges under any *long-term insurance contracts*);

(6) the formal wordings of *reinsurance* contracts; and

(7) any other relevant information on the *firm's reinsurance* or other risk-transfer arrangements, including the extent to which they:

(a) have been exhausted by recoveries on paid *claims*; and

(b) will be exhausted by recoveries on reported *claims* and, to the extent known, on incurred but not reported *claims*.

17.1.39 G A *firm* should retain its underwriting and *claims* histories for as long as they may be needed to inform pricing or provisioning decisions.

18 Guidance on Public Interest Disclosure Act: whistleblowing

18.1 Application

18.1.1 G This chapter is relevant to every *firm* to the extent that the Public Interest Disclosure Act 1998 ("PIDA") applies to it.

Purpose

18.1.2 G (1) The purposes of this chapter are:

(a) to remind *firms* of the provisions of PIDA; and

(b) to encourage *firms* to consider adopting and communicating to workers appropriate internal procedures for handling workers' concerns as part of an effective risk management system.

(2) In this chapter "worker" includes, but is not limited to, an individual who has entered into a contract of employment.

18.1.3 G The *guidance* in this chapter concerns the effect of PIDA in the context of the relationship between *firms* and the *FSA*. It is not comprehensive guidance on PIDA itself.

18.2 Practical measures

Effect of Public Interest Disclosure Act 1998

18.2.1 G (1) Under PIDA, any clause or term in an agreement between a worker and his employer is void in so far as it purports to preclude the worker from making a protected disclosure (that is, "blow the whistle").

(2) In accordance with section 1 of PIDA:

(a) a protected disclosure is a qualifying disclosure which meets the relevant requirements set out in that section;

(b) a qualifying disclosure is a disclosure, made in good faith, of information which, in the reasonable belief of the worker making the disclosure, tends to show that one or more of the following (a "failure") has been, is being, or is likely to be, committed:

(i) a criminal offence; or

(ii) a failure to comply with any legal obligation; or

(iii) a miscarriage of justice; or

(iv) the putting of the health and safety of an individual in danger; or

(v) damage to the environment; or

(vi) deliberate concealment relating to any of (i) to (v);

it is immaterial whether the relevant failure occurred, occurs or would occur in the *United Kingdom* or elsewhere, and whether the law applying to it is that of the *United Kingdom* or of any other country or territory.

Internal procedures

18.2.2 G (1) *Firms* are encouraged to consider adopting (and encouraged to invite their *appointed representatives* to consider adopting) appropriate internal procedures which will encourage workers with concerns to blow the whistle internally about matters which are relevant to the functions of the *FSA*.

(2) Smaller *firms* may choose not to have as extensive procedures in place as larger *firms*. For example, smaller *firms* may not need written procedures. The following is a list of things that larger and smaller *firms* may want to do.

(a) For larger *firms*, appropriate internal procedures may include:

(i) a clear statement that the *firm* takes failures seriously (see *SYSC* 18.2.1G(2)(b));

(ii) an indication of what is regarded as a failure;

(iii) respect for the confidentiality of workers who raise concerns, if they wish this;

(iv) an assurance that, where a protected disclosure has been made, the *firm* will take all reasonable steps to ensure that no *person* under its control engages in victimisation;

(v) the opportunity to raise concerns outside the line management structure, such as with the Compliance Director, Internal Auditor or Company Secretary;

(vi) penalties for making false and malicious allegations;

(vii) an indication of the proper way in which concerns may be raised outside the *firm* if necessary (see (3));

(viii) providing access to an external body such as an independent charity for advice;

(ix) making whistleblowing procedures accessible to staff of key contractors; and

(x) written procedures.

(b) For smaller *firms*, appropriate internal procedures may include:

(i) telling workers that the *firm* takes failures seriously (see *SYSC* 18.2.1G(2)(b)) and explaining how wrongdoing affects the organisation;

(ii) telling workers what conduct is regarded as failure;

(iii) telling workers who raise concerns that their confidentiality will be respected, if they wish this;

(iv) making it clear that concerned workers will be supported and protected from reprisals;

(v) nominating a senior officer as an alternative route to line management and telling workers how they can contact that individual in confidence;

(vi) making it clear that false and malicious allegations will be penalised by the *firm*;

(vii) telling workers how they can properly blow the whistle outside the *firm* if necessary (see (3));

(viii) providing access to an external body for advice such as an independent charity for advice; and

(ix) encouraging managers to be open to concerns.

(3) (a) *Firms* should also consider telling workers (through the *firm's* internal procedures, or by means of an information sheet available from the *FSA's* website, or by some other means) that they can blow the whistle to the *FSA*, as the regulator prescribed in respect of financial services and markets matters under PIDA.

(b) The *FSA* will give priority to live concerns or matters of recent history, and will emphasise that the worker's first port of call should ordinarily be the *firm* (see Frequently Asked Questions on http://www.fsa.gov.uk/Pages/Doing/Contact/Whistle/FAQ/index.shtml).

(c) For the *FSA's* treatment of confidential information, see *SUP* 2.2.4G.

Link to fitness and propriety

18.2.3 G The *FSA* would regard as a serious matter any evidence that a *firm* had acted to the detriment of a worker because he had made a protected disclosure (see *SYSC* 18.2.1G(2)) about matters which are relevant to the functions of the *FSA*. Such evidence could call into question the fitness and propriety of the *firm* or relevant members of its staff, and could therefore, if relevant, affect the *firm's* continuing satisfaction of *threshold condition* 5 (Suitability) or, for an *approved person*, his status as such.

Annex F

Senior Management Arrangements, Systems and Controls Handbook (SYSC) coming into force on 1 November 2007

In this Annex, underlining indicates new text and striking through indicates deleted text. In this Annex where an entire section is being deleted, the place where the change will be made is indicated and the text will not be struck through.

Amend SYSC 1.1 as follows

1.1 Application of SYSC 2 and SYSC 3

….

1.1.1 R Who?

SYSC 2 and *SYSC* 3 apply to every *firm* except that:

…

(6) ~~*SYSC* 3.2.23R to *SYSC* 3.2.36R apply only to a *BIPRU firm*~~ for a *common platform firm*, *SYSC* 3 does not apply.

…

~~1.3.1A G From 1 January 2007 until 1 November 2007, the application of the *common platform requirements* is limited by *SYSC* TP 1.~~[deleted]

…

1.3.4 R ~~[To follow.]~~ The provisions on record-keeping in *SYSC* 9 apply as set out in *SYSC* 1.3.2R, except that they only apply to the carrying on of *ancillary activities* that are performed in relation to:

(1) *designated investment business*;

(2) *home finance activity*; and

(3) *insurance mediation activity*.

…

Amend SYSC 3 as follows

…

3.1.1A	R	[deleted]

…

3.2.23R	R	[deleted]
3.2.24	R	[deleted]
3.2.25	R	[deleted]
3.2.26	R	[deleted]
3.2.27	R	[deleted]
3.2.28	R	[deleted]
3.2.29	R	[deleted]
3.2.30	R	[deleted]
3.2.31	R	[deleted]
3.2.32	R	[deleted]
3.2.33	R	[deleted]
3.2.34	R	[deleted]
3.2.35	R	[deleted]
3.2.36	R	[deleted]

Amend SYSC 12 as follows

…

12.1.13	R	If this *rule* applies under *SYSC* 12.1.14R to a *firm*, the *firm* must:
		(1) …; and
		(2) ensure that the risk management processes and internal control mechanisms at the level of any *UK consolidation group* or *non-EEA sub-group* of which it is a member comply with the obligations set out in the following provisions on a consolidated (or sub-consolidated) basis:

(a) ~~*SYSC* 3.2.23R and *SYSC* 3.2.24R~~ *SYSC* 4.1.1R and *SYSC* 4.1.2R;

(b) ~~*SYSC* 3.2.26R~~ *SYSC* 4.1.7R;

(c) ~~*SYSC* 3.2.28R to *SYSC* 3.2.36R~~ *SYSC* 5.1.7R;

(d) ~~*SYSC* 11.1.11R and *SYSC* 11.1.12R~~ *SYSC* 7;

(e) ~~*BIPRU* 2.3.7R(1)~~ *SYSC* 11.1.11R and *SYSC* 11.1.12R;

(f) ~~*BIPRU* 9.1.6R *and BIPRU* 9.13.21R (Liquidity plans)~~ *BIPRU* 2.3.7R(1);

(g) ~~*BIPRU* 10.12.3R (Concentration risk policies)~~ *BIPRU* 9.1.6R and *BIPRU* 9.13.21R (Liquidity plans);

(h) *BIPRU* 10.12.3R (Concentration risk policies).

Annex G

Principles for Businesses sourcebook (PRIN)

In this Annex, underlining indicates new text and striking through indicates deleted text.

…

1.2.5 G A *firm* is therefore not required to classify its *clients* (because *COB* 4.1.4 R does not apply) and may choose to comply with *Principles* 6, 7, 8 and 9 as if all its *clients* were *customers*. Alternatively, it may choose to distinguish between *market counterparties* and *customers* in complying with those *Principles*. But, in that case, the *firm* would need to classify any *client* treated as a *market counterparty*. In doing this, the requirements in *SYSC* will apply, including the requirement to establish appropriate systems and controls ~~*SYSC* 3.1.1 R)~~ and the requirement to make and retain adequate records ~~*SYSC* 3.2.20 R)~~. In classifying its *market counterparties*, it would be open to such a *firm*, although not obligatory, to permit *intermediate customers* to opt up to *market counterparty* status in accordance with *COB* 4.1.12 R. It would also have to treat a *market counterparty* as a *customer* if the *firm* had chosen to treat the *client* as a *private customer* in the circumstances set out in *COB* 4.1.14 R.

…

Annex H

Threshold Conditions (COND)

In this Annex, underlining indicates new text and striking through indicates deleted text.

…

2.4.4(2) G (2) …

(d) whether the *firm* has taken reasonable steps to identify and measure any risks of regulatory concern that it may encounter in conducting its business (see *COND* 2.4.6 G) and has installed appropriate systems and controls and appointed appropriate human resources to measure them prudently at all times; see *SYSC* 3.1 (Systems and Controls), ~~and~~ *SYSC* 3.2 (Areas covered by systems and controls) and *SYSC* 4.1.1R (Organisational requirements); and

…

2.4.5 G In complying with *SYSC* ~~3.1.1 R~~ (Systems and controls), a *firm* should plan its business appropriately so that it is able to identify, measure and manage the likely risks of regulatory concern it will face (*SYSC* 3.2.17 G (Business strategy) and *SYSC* 7 (Risk control)).

…

2.4.6 G (3) The *FSA* would expect the level of detail in a *firm*'s business plan or strategy plan in (2) to be appropriate to the complexity of the *firm*'s proposed *regulated activities* and *unregulated activities* and the risks of regulatory concern it is likely to face (see *SYSC* 3.2.11 G (Management information) and *SYSC* 7 (Risk control). Notes on the contents of a business plan are given in the business plan section of the application pack for *Part IV permission*. A *firm* requiring specific *guidance* on the contents and level of detail of its business plan should contact the Corporate Authorisation department (see *AUTH* 3: Applications for *Part IV permission*), or, if relevant, its usual supervisory contact at the *FSA*, or seek professional assistance.

…

2.5.6 G In determining whether a *firm* will satisfy, and continue to satisfy, threshold condition 5 in respect of conducting its business with integrity and in compliance with proper standards, the relevant matters, as referred to in *COND* 2.5.4 G (2), may include but are not limited to whether:

…

(6) the *firm* has taken reasonable care to establish and maintain effective systems and controls for compliance with applicable requirements

and standards under the regulatory system that apply to the *firm* and the *regulated activities* for which it has, or will have, permission (see *SYSC* 3.2.6 R to *SYSC* 3.2.8 R (Compliance) and *SYSC* 6.1.1 to *SYSC* 6.1.5);

…

2.5.7 G In determining whether a *firm* will satisfy and continue to satisfy threshold condition 5 in respect of having competent and prudent management and exercising due skill, care and diligence, relevant matters, as referred to in *COND* 2.5.4 G (2), may include, but are not limited to whether:

…

(3) the *governing body* of the *firm* is organised in a way that enables it to address and control the *regulated activities* of the *firm*, including those carried on by *managers* to whom particular functions have been delegated (see *SYSC* 2.1 (Apportionment of responsibilities) and *SYSC* 3.2 (Areas covered by systems and controls) and *SYSC* 4.1.1 (General organisational requirements));

…

(5) the *firm* has made arrangements to put in place an adequate system of internal control to comply with the requirements and standards under the *regulatory system* (see *SYSC* 3.1 (Systems and Controls) and *SYSC* 4.1 (General organisational requirements));

(6) the *firm* has approached the control of financial and other risk in a prudent manner (for example, by not assuming risks without taking due account of the possible consequences) and has taken reasonable care to ensure that robust information and reporting systems have been developed, tested and properly installed (see *SYSC* 3.2.10G (Risk assessment) and *SYSC* 7.1 (Risk control));

…

(8) the *firm* has developed human resources policies and procedures that are reasonably designed to ensure that it employs only individuals who are honest and committed to high standards of integrity in the conduct of their activities (see, for example, *SYSC* 3.2.13G (Employees and agents) and *SYSC* 5.1 (Employees, agents and other relevant persons));

…

(10) the *firm* has in place systems and controls against *money laundering* of the sort described in *SYSC* 3.2.6 R to *SYSC* 3.2.6J G and *SYSC* 6.3 (Financial crime);

Annex I

Conduct of Business sourcebook (COB)

In this Annex, underlining indicates new text and striking through indicates deleted text.

…

2.4.1A	R		This section does not apply to a *common platform firm* if *SYSC* 10.2 (Chinese walls) applies to the *firm*.

…

5.10.1A	R		This section does not apply to a *common platform firm* if *SYSC* 10.1 (conflicts of interest) applies to the *firm*.

….

Application

7.1.1	R	(1)	This section applies to a *firm* when it is conducting *designated investment business* with or for a *customer*.
		(2)	*COB* 7.1.4 E (1) do not apply in relation to *investment research* (see COB 7.3 (Dealing ahead of investment research)).
		(3)	This section does not apply to a *common platform firm* if *SYSC* 10.1 (conflicts of interest) applies to the *firm*.

Annex J

Insurance: Conduct of Business sourcebook (ICOB)

In this Annex, underlining indicates new text and striking through indicates deleted text.

…

1.2.2 G …

(3) *Firms* which outsource *regulated activities* are reminded of the *guidance* on *outsourcing* in *SYSC* 3.2.4 G and the *rules* in *SYSC* 8.

…

7.4.7A R *ICOB* 7.4.5R to *ICOB* 7.4.7G do not apply to a *common platform firm* if *SYSC* 10.1 (conflicts of interest) applies to the *firm*.

…

Summary of Handbook provisions for insurance intermediaries

Annex 2	High level standards	Senior management arrangements, Systems and Controls, *SYSC*	Applies in respect of (1) and (2), except *SYSC* 3.2.6A R to *SYSC* 3.2.6J G1 and *SYSC* 4-10

…

…

3.3.9 G (1) A *firm* is reminded that *non-investment financial promotions* (including those which are exempt) may be subject to more general *rules* including *Principle* 7 (Communications with clients), *SYSC* ~~3~~ (Systems and controls) *ICOB* 2.2.3 R (Clear, fair and not misleading communication) and *ICOB* 5 (Product disclosure).

…

Annex K

Mortgages: Conduct of Business sourcebook (MCOB)

In this Annex, underlining indicates new text and striking through indicates deleted text.

…

1.2.1A G *Firms* which outsource *regulated activities* are reminded of the *guidance* on *outsourcing* in *SYSC* 3.2.4G and *SYSC* 8.

…

3.2.8 G *Firms* are reminded that *qualifying credit promotions* (including those which are exempt) may be subject to more general *rules*, including *Principle* 7 (Communications with clients), *SYSC* 3 to *SYSC* 10 (Systems and controls) and *MCOB* 2.2.6 R (Clear, fair and not misleading communication).

…

4.3.3 G *SYSC* 3.2.6 R and *SYSC* 6.1.1R (Compliance) require a *firm* (including a *common platform firm)* to 'take reasonable care to establish, implement and maintain effective systems and controls for compliance with applicable requirements and standards under the *regulatory system*'. In meeting this requirement in relation to *MCOB* 4.3.2 R , a *firm* which states that it provides a service based on a limited number of *mortgage lenders* (see *MCOB* 4.3.1 R (1)(b)) should have adequate systems and controls in place to monitor whether business is actually placed with those *mortgage lenders.*

…

13.3.8 G *Firms* that propose to outsource aspects of *customer* relationships (including debt collection) should note that, as set out in *SYSC* 3.2.4 G(1) and *SYSC* 8, the *FSA* will continue to hold them responsible for the way in which this work is carried on.

…

Annex L

Client Assets sourcebook (CASS)

In this Annex, underlining indicates new text and striking through indicates deleted text.

…

2.2.20 G A *firm* that holds *safe custody investments* with a *custodian* or *recommends custodians* to *private customers*, is expected to establish and maintain a system for assessing the appropriateness of its selection of the *custodian* and to assess the continued appointment of that *custodian* periodically as often as is reasonable in the relevant market. In order to comply with *SYSC* 3.2.20R and *SYSC* 9 (Records), the *firm* is also expected to make and retain a record of the grounds on which it satisfies itself as to the appropriateness of its selection or, following a periodic assessment, continued appropriateness of the *custodian*.

…

Annex M

Market Conduct sourcebook (MAR)

In this Annex, underlining indicates new text and striking through indicates deleted text.

…

3.6.1 G (1) …

(2) *MAR* 3.6 also provides additional *guidance* on the record-keeping requirements of *SYSC* 3.2.20R and *SYSC* 9 (Records).

…

3.6.6 G If the records identified in *MAR* 3.6.3G are substituted by written or electronic confirmations produced in accordance with *SYSC* 3.2.20 R and *SYSC* 9 (Records), then that confirmation may be an adequate record of the transaction.

…

Annex N

Training and Competence sourcebook (TC)

In this Annex, underlining indicates new text and striking through indicates deleted text.

...

1.1.4 G *Principle* 3 is amplified in *SYSC*. A *firm* must take reasonable care to establish and maintain such systems and controls as are appropriate to its business (*SYSC* 3.1.1R and *SYSC* 4.1.1R to *SYSC* 4.1.5R). Also, a *firm's* systems and controls should enable it to satisfy itself of the suitability of anyone who acts for it (*SYSC* 3.2.13G and *SYSC* 5.1.2G). This would include the competence of the individual for the role.

Annex O

Supervision manual (SUP)

In this Annex, underlining indicates new text and striking through indicates deleted text.

…

Rules which can be waived (see SUP 8.2.6 G)

8.2.7	G	Rules	Section of the Act or other provision under which rules are made	Chapters of the Handbook where such rules appear (Note 1)
		…		
		Money laundering rules	Section 146	*SYSC* 3.2 and *SYSC* 6.3

…

10.7.13A	G	A *firm's* obligations in respect of its *money laundering reporting officer* are set out in *SYSC* 3.2.6I R and *SYSC* 6.3.9R.

…

10.12.3	G	… See also *SYSC* 3.2.4G and *SYSC* 8.1.1R, and for *insurers SYSC* ~~3A.9~~ 13.9.

10.12.4	G	*Outsourcing arrangements*		*Submitting form*
		…		
		(i) …	Responsibility for (as opposed to the performance of) any activity *outsourced* to B will remain with A. See *SYSC* 3.2.4G and *SYSC* 8	

12.6.7	G	The senior management of a *firm* should be aware that the activities of *appointed representatives* are an integral part of the business that they manage. The responsibility for the control and monitoring of the activities of *appointed representatives* rests with the senior management of the *firm*. *Guidance* is set out in *SYSC* ~~*SYSC* 3~~ on delegation ~~(for example, *SYSC SYSC* 3.2.3 G and *SYSC* 3.2.4 G)~~ and in the *Statements of Principle* and *Code of Practice for Approved Persons* in *APER* (for example, *APER* 4.5 and *APER* 4.6).

…

Application of the handbook to incoming EEA firms

13A Annex 1	G	(1) Module of Handbook	(2) Potential application to an incoming EEA firm with respect to activities carried on from an establishment of the firm (or its appointed representative) in the United Kingdom	(3) Potential application to an incoming EEA firm with respect to activities carried on other than from an establishment of the firm (or its appointed representative) in the United Kingdom
		…		
		SYSC	*SYSC* 1 contains application provisions only. *SYSC* 2 and *SYSC* 3 apply as set out in *SYSC* 1.1.1 R (1): (1) *SYSC* 2.1.1 R (1) and *SYSC* 2.1.2 G do not apply; (2) … (3) *SYSC* 3 applies, but only in so far as responsibility for the matter in question is not reserved by a European Community instrument to the *firm's Home State regulator*. *SYSC* 1.1.7 R (Where?) further restricts the territorial application of *SYSC* 1 to *SYSC* 3 for an *incoming EEA firm*. Further *guidance* is contained in *SYSC* 2.1.6 G, Question 12. ~~*SYSC* 4~~ *SYSC* 18 applies to the extent that the Public Interest Disclosure Act 1998 applies to the *firm*.	…

Annex P

Enforcement manual (ENF)

In this Annex, underlining indicates new text and striking through indicates deleted text.

…

11.5.2 G However, in some cases, it will not be appropriate to take disciplinary measures against a *firm* for the actions of an *approved person* (for example, if the *firm* can show that it took all reasonable steps to prevent the breach). In other cases, it may be appropriate for the *FSA* to take action against both the *firm* and the *approved person*. For example, a *firm* may have breached the rule requiring it to take reasonable care to establish and maintain such systems and controls as are appropriate to its business *SYSC* 3.1.1 R or *SYSC* 4.1.1R), and an *approved person* may have taken advantage of those deficiencies to front run orders or misappropriate assets.

…

11.7.1 G In a number of circumstances the *regulatory system* requires a *firm* to take reasonable care in relation to particular behaviour. For example, *Principle* 3 requires a *firm* to take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems, and *SYSC* 3.1.1 R (taken with *SYSC* 3.1.2 G) and *SYSC* 4.1.1R (taken with 4.1.2G) requires a *firm* to take reasonable care to establish and maintain such systems and controls as are appropriate to the nature, scale and complexity of its business.

…

11.9.1 G The *FSA*'s money laundering *rules* are set out in *SYSC* 3.2 and *SYSC* 6.3 (Financial crime) The *FSA*, when considering whether to take disciplinary action in respect of a breach of those *rules*, will have regard to whether a *firm* has followed relevant provisions in the Joint Money Laundering Steering Group's Guidance Notes for the Financial Sector.

Annex Q

Credit Unions sourcebook (CRED)

In this Annex, underlining indicates new text and striking through indicates deleted text.

…

4.1.3 G *SYSC* 1 to *SYSC* 3 apply to all *credit unions* in respect of the carrying on of their *regulated activities* and *unregulated activities* in a *prudential context*. ~~*SYSC* 4~~ *SYSC* 18 applies to all *credit unions* without restriction.

…

4.1.8 G ~~*SYSC* 4~~ *SYSC* 18 *reminds firms* of the provisions of the Public Interest Disclosure Act 1998 and encourages them to consider adopting appropriate internal whistleblowing procedures. This applies equally to *credit unions* but is not the subject of further *guidance* in this chapter.

…

Annex R

Professional Firms sourcebook (PROF)

In this Annex, underlining indicates new text and striking through indicates deleted text.

…

5.3.4	G	*SYSC* 3.2.6A R to *SYSC* 3.2.6J G and *SYSC* 6.3 (Financial crime), in relation to *money laundering*, do not apply to *authorised professional firms* when carrying on *non-mainstream regulated activities*.

…

Annex S

Recognised Investment Exchanges and Recognised Clearing Houses sourcebook (REC)

In this Annex, underlining indicates new text and striking through indicates deleted text.

…

2.5A.6	G	(2)	In considering appropriate internal procedures, *UK recognised bodies* may find the *guidance* provided to *firms* in *SYSC* 18.2.2G(2) and (3) ~~4.2.2 G(2) and (3)~~ helpful.

…

Annex T

Glossary of Definitions

In this Annex, underlining indicates new text and striking through indicates deleted text.

ancillary service	any of the services listed in Section B of Annex I to *MiFID*.	
broker	(in *MAR*, *SYSC* and *INSPRU*) any person when dealing as agent.	
collateral	(2)	…
	(3)	(in *INSPRU* and *SYSC*)
		(a) …
CRD	the *Capital Adequacy Directive* and the *Banking Consolidation Directive*.	
client	(1)	(except in *PROF*, in relation to a *regulated mortgage contract* and *SYSC* 10) any *person* with or for whom a *firm* conducts or intends to conduct *designated investment business* or any other *regulated activity*; and:
	…	
	(3A)	(in *SYSC* 10) any *person* to whom a *common platform firm* provides, or intends to provide, a service in the course of carrying on a *regulated activity* for that *person*, but does not include:
		(a) a trust beneficiary; or
		(b) a *corporate finance contact*; or
		(c) a *venture capital contact*;
	(4)	(in relation to a *regulated mortgage contract*, except in *PROF* and SYSC 10) the individual or trustee who is the borrower or potential borrower under that contract.
common platform firm	a *firm* that is:	
	(a)	a *BIPRU firm*; or
	(b)	an *exempt CAD firm*; or
	(c)	a UK *MiFID investment firm* which falls within the definition of 'local firm' in article 3.1P of the *Capital Adequacy Directive*.

common platform organisational requirements	*SYSC* 4 to *SYSC* 9.
common platform record-keeping requirements	*SYSC* 9.
common platform requirements	*SYSC* 4 to *SYSC* 10.
common platform requirements on financial crime	*SYSC* 6.3.
competent authority[1]	(1) (in relation to ~~the functions referred to in Part VI of the *Act*'~~ admission to an *official listing*): (a) the authority designated under Schedule 8 to the *Act* (Transfer of functions under Part VI (Official listing)) as responsible for ~~performing those functions under the *Act*~~ admitting securities to, and for removing securities from, the *official list*; for the time being, the *FSA* in its capacity as such; or (b) an authority exercising functions corresponding to those ~~functions under the laws of~~ in (a) in another *EEA State*. (2) (in relation to the exercise of an *EEA right*) a competent authority for the purposes of the relevant *Single Market Directive*. (3) …
conflicts of interest policy	the policy established and maintained in accordance with *SYSC* 10.1.10R.
control	(1) (except for a *common platform firm*) (in relation to the acquisition, increase or reduction of control of a *firm*) the relationship between a *person* and the *firm* or other *undertaking* of which the *person* is a controller. (2) (for a *common platform firm*) control as defined in article 1 of Directive 83/349/EEC. [Note: article 4 (1)(30) of *MiFID*]

[1] This definition is based on the definition contained in the CRD (Consequential Amendments) Instrument 2006 which was consulted on in the consultation paper Strengthening Capital Standards 2 (CP 06/3)

durable medium	(a)	paper; or
	(b)	~~(in accordance with article 2(f) of the *Distance Marketing Directive* and article 2(12) of the *Insurance Mediation Directive*)~~ any instrument which enables the recipient to store information addressed personally to him in a way accessible for future reference for a period of time adequate for the purposes of the information and which allows the unchanged reproduction of the information stored; this includes, in particular, floppy disks, CD-ROMs, DVDs and the hard drive of the recipient's computer on which the electronic mail is stored, but not Internet websites unless they fulfill the criteria in this definition. (in relation to *MiFID business* or *equivalent business of a third country investment firm*, if the relevant *rule* implements the *MiFID implementing Directive*) the instrument used must be: (i) appropriate to the context in which the business is to be carried on; and (ii) chosen by the *consumer* when offered the choice between that instrument and paper. [Note: article 2(f) and Recital 20 of the *Distance Marketing Directive*, article 2(12) of the *Insurance Mediation Directive* and article 2(2) of the *MiFID implementing Directive*]
eligible counterparty	means a *market counterparty*.	
equivalent business of a third country investment firm	the business of a *third country investment firm* carried on from an establishment in the *United Kingdom* that would be *MiFID business* if that firm were a *MiFID investment firm*.	
financial instrument	…	
	(2)	(for the purposes of *BIPRU* and *GENPRU*) an instrument listed in Section B of the Annex to the *ISD*; and
	(3)	(for the *common platform requirements*) any of the instruments specified in Section C of Annex I of *MiFID*.
group	…	
	(5)	(in relation to a *common platform firm*) means the group of which that *firm* forms a part, consisting of a parent undertaking, its subsidiaries and the entities in which the parent undertaking or its subsidiaries hold a participation, as well as undertakings linked to each other by a relationship within the meaning of article 12(1) of

	Directive 83/349/EEC on consolidated accounts. [Note: article 2(5) of the *MiFID implementing Directive*]
investment service	(1) … (2) (for the *common platform requirements*) any of the services and activities listed in Section A of Annex 1 to *MiFID* involving the provision of a service in relation to a *financial instrument*.
investment services and activities; or *investment services or activities*; or *investment services and/or activities*	any of the services and activities listed in Section A of Annex I to *MiFID* relating to any *financial instrument*.
MiFID	The European Parliament and Council Directive on markets in financial instruments (No. 2004/39/EC). See also *MiFID Regulation* and *MiFID implementing Directive*.
MiFID business	*investment services and activities* and, where relevant, *ancillary services* carried on by a *MiFID investment firm*.
MiFID implementing Directive	Commission Directive No. 2006/73/EC implementing Directive 2004/39/EC of the European Parliament and of the Council as regards organisational requirements and operating conditions for investment firms and defined terms for the purposes of that Directive.
MiFID investment firm	(in summary) a *firm* to which *MiFID* applies including, for some purposes only, a *credit institution* and *UCITS investment firm*. (in full) a *firm* which is: (1) an *investment firm* with its head office in the *EEA* (or, if it has a registered office, that office); (2) a *BCD credit institution* (only when providing an *investment service or activity* in relation to the *rules* implementing the articles referred to in article 1(2) of *MiFID*); (3) a *UCITS investment firm* (only when providing the services referred to in article 5(3) of the *UCITS Directive* in relation to the *rules* implementing the articles of *MiFID* referred to in article 5(4) of that Directive);

	unless, and to the extent that, *MiFID* does not apply to it as a result of article 2 (Exemptions) or article 3 (Optional exemptions) of *MiFID*.
MiFID Regulation	Commission Regulation (EC) 1287/2006 implementing Directive 2004/39/EC of the European Parliament and of the Council as regards organisational requirements and operating conditions for investment firms and defined terms for the purposes of that Directive
outsourcing	(1) (except in *SYSC* 8) the use of a *person* to provide customised services to a *firm* other than: (a) a member of the *firm's* governing body acting in his capacity as such; or (b) an individual employed by a *firm* under a contract of service. (2) (in *SYSC* 8) an arrangement of any form between a *firm* and a service provider by which that service provider performs a process, a service or an activity which would otherwise be undertaken by the *firm* itself. [Note: article 2(6) of the *MiFID implementing Directive*]
professional client	means an *intermediate customer*.
regulatory system	the arrangements for regulating a *firm* or other *person* in or under the *Act*, including the *threshold conditions*, the *Principles* and other *rules*, the *Statements of Principle*, codes and *guidance* and including any relevant directly applicable provisions of a European Regulation such as those contained in the *MiFID Regulation*.
relevant person	(1) (in *COMP*) a *person* for *claims* against whom the *compensation scheme* provides cover, as defined in *COMP* 6.2.1R. (2) any of the following: (a) a *director*, *partner* or equivalent, manager or *appointed representative* (or where applicable, *tied agent*) of the *firm*; (b) a *director*, *partner* or equivalent, or manager of any *appointed representative* (or where applicable, *tied agent*) of the *firm*; (c) an *employee* of the *firm* or of an *appointed representative* (or where applicable, *tied agent*) of the *firm*; as well as any other natural person whose

	services are placed at the disposal and under the control of the *firm* or a *tied agent* of the *firm* and who is involved in the provision by the *firm* of *regulated activities*;
	(d) a natural person who is involved in the provision of services to the *firm* or its *appointed representative* (or where applicable, *tied agent*) under an *outsourcing* arrangement for the purpose of the provision by the *firm* of *regulated activities*.
	[Note: article 2(3) of the *MiFID implementing Directive*]
retail client	means a *private customer*.
senior personnel	those *persons* who effectively direct the business of the *firm*, which could include a *firm's governing body* and other *persons* who effectively direct the business of the *firm*.
supervisory function	any function within a *common platform firm* that is responsible for the supervision of its *senior personnel*.
third country investment firm	a *firm* which would be a *MiFID investment firm* if it had its head office in the *EEA*.
tied agent	a *person* who, under the full and unconditional responsibility of only one *MiFID investment firm* on whose behalf it acts, promotes *investment services* and/or *ancillary services* to *clients* or prospective *clients*, receives and transmits instructions or orders from the *client* in respect of *investment services* or *financial instruments*, places *financial instruments* and/or provides *investment advice* to *clients* or prospective *clients* in respect of those *financial instruments* or *investment services.* [Note: article 4(1)(25) of *MiFID*]