Chapter 7

Risk control

7.1 Risk control

[Note: ESMA has also issued guidelines under article 16(3) of the ESMA Regulation covering certain aspects of the MiFID compliance function requirements. See http://www.esma.europa.eu/content/Guidelines-certain-aspects-MiFID-compliance-function-requirements .]

Application to a common platform firm

7.1.-2 G For a *common platform firm*:

(1) the *MiFID Org Regulation* applies, as summarised in ■ SYSC 1 Annex 1 3.2G, ■ SYSC 1 Annex 1 3.2-AR and ■ SYSC 1 Annex 1 3.2-BR; and

(2) the *rules* and *guidance* apply as set out in the table below:

Subject	Applicable rule or guidance
Risk assessment	SYSC 7.1.1G
Risk management	SYSC 7.1.4R, SYSC 7.1.4AG
Risk control: remuneration	SYSC 7.1.7BG, SYSC 7.1.7BBG
Risk control: additional provisions	SYSC 7.1.7CG, SYSC 7.1.8G, SYSC 7.1.9R to SYSC 7.1.16R
Additional rules for CCR firms	SYSC 7.1.16CR to SYSC 7.1.22R

Application to an MiFID optional exemption firm and to a third country firm

7.1.-1 G For a *MiFID optional exemption firm* and a *third country firm*:

(1) the *rules* and *guidance* in this chapter apply to them as if they were *rules* or as *guidance* in accordance with ■ SYSC 1 Annex 1 3.2CR(1); and

(2) those articles of the *MiFID Org Regulation* in ■ SYSC 1 Annex 1 2.8AR and 3.2CR apply to them as if they were *rules* or as *guidance* in accordance with ■ SYSC 1 Annex 1 3.2CR(2).

Risk assessment

7.1.1 G ■ SYSC 4.1.1 R requires a *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 *UCITS investment 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*.

7.1.2A G Other *firms* should take account of the risk management policies and procedures *rule* (■ SYSC 7.1.2 R) as if it were *guidance* (and as if should appeared in that *rule* instead of must) as explained in ■ SYSC 1 Annex 1 3.3 R(1).

7.1.2B G A *management company* should be aware that ■ COLL 6.11 contains requirements implementing article 12 of the *UCITS implementing Directive* in relation to risk control and internal reporting that will apply to it.

7.1.2C G *Full-scope UK AIFMs* should be aware that ■ FUND 3.7 and articles 38 to 47 of the *AIFMD level 2 regulation* contain further requirements in relation to risk management.

7

Risk management

7.1.3 R A *UCITS investment 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.

7.1.4 R The *management body* 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**: article 76(1) of *CRD*]

7.1.4A G For a *common platform firm* included within the scope of ■ SYSC 20 (Reverse stress testing), the strategies, policies and procedures for identifying, taking up, managing, monitoring and mitigating the risks to which the *firm* is or might be exposed include conducting reverse stress testing in accordance with ■ SYSC 20. A *common platform firm* which falls outside the scope of ■ SYSC 20 should consider conducting reverse stress tests on its business plan as well. This would further *senior personnel's* understanding of the *firm's* vulnerabilities and would help them design measures to prevent or mitigate the risk of business failure.

7.1.4B G Other *firms* should take account of the risk management *rules* (■ SYSC 7.1.3 R and ■ SYSC 7.1.4 R) as if they were *guidance* (and as if "should" appeared in those *rules* instead of "must") as explained in ■ SYSC 1 Annex 1 3.3 R(1).

7.1.5 R A *UCITS investment 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 7.1.3 R;

(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.

7.1.6 R A *UCITS investment 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 7.1.2 R to ■ SYSC 7.1.5 R; and

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

7.1.7 R Where a *UCITS investment firm* is not required under ■ SYSC 7.1.6 R 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 7.1.2 R to ■ SYSC 7.1.5 R satisfy the requirements of those *rules* and are consistently effective.

7.1.7A G Other *firms* should take account of the risk management *rules* (■ SYSC 7.1.5 R to ■ SYSC 7.1.7 R) as if they were *guidance* (and as if should appeared in those *rules* instead of must) as explained in ■ SYSC 1 Annex 1 3.3 R(1).

7.1.7B G In setting the method of determining the *remuneration* of *employees* involved in the risk management function:

(1) *firms* that ■ SYSC 19D applies to will also need to comply with the *dual-regulated firms Remuneration Code*; and

(2) *firms* that the remuneration part of the *PRA Rulebook* applies to will also need to comply with it.

7.1.7BA G In setting the method of determining the *remuneration* of *employees* involved in the risk management function *full-scope UK AIFMs* will need to comply with the *AIFM Remuneration Code*.

7.1.7BB G In setting the method of determining the *remuneration* of *employees* involved in the risk management function, *BIPRU firms* will also need to comply with the *BIPRU Remuneration Code*.

7.1.7BC G In setting the method of determining the *remuneration* of *employees* involved in the risk management function, *firms* that ■ SYSC 19A applies to will also need to comply with the *Remuneration Code*.

Risk control: additional provisions

7.1.7C G *Firms* should also consider the additional *guidance* on risk-centric governance arrangements for effective risk management contained in ■ SYSC 21.

7.1.8 G (1) [deleted]

(2) The term 'risk management function' in ■ SYSC 7.1.6 R and ■ SYSC 7.1.7R, and for a *common platform firm* in article 23(2) of the *MiFID Org Regulation*, refers to the generally understood concept of risk assessment within a *firm*, that is, the function of setting and controlling risk exposure.

(3) For a *firm* that is not a *relevant authorised person*, the risk management function is not a *controlled function* itself, but is part of the *systems and controls function* or the *PRA*'s systems and controls *controlled function* (CF28).

(4) For a *relevant authorised person*, the risk management function is a *PRA controlled function* (SMF4).

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

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.

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

7.1.12 G The documentation maintained by a *BIPRU firm* under ■ SYSC 4.1.3 R 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.

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.

Interest rate risk

7.1.15 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.

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.

7.1.16A G [deleted]

7.1.16B G [deleted]

Additional rules for CRR firms

7.1.16C R In ■ SYSC 7.1.18 R a '*CRR firm*' that is significant' means a significant *IFPRU firm*.

7.1.17 R

(1) The *management body* of a *CRR firm* has overall responsibility for risk management. It must devote sufficient time to the consideration of risk issues.

(2) The *management body* of a *CRR firm* must be actively involved in and ensure that adequate resources are allocated to the management of all material risks addressed in the rules implementing the *CRD* and in the *EU CRR* as well as in the valuation of assets, the use of external ratings and internal models related to those risks.

(3) A *CRR firm* must establish reporting lines to the *management body* that cover all material risks and risk management policies and changes thereof.

[**Note**: article 76(2) of *CRD*]

7.1.18 R

(1) A *CRR firm* that is significant must establish a risk committee composed of members of the *management body* who do not perform any executive function in the firm. Members of the risk committee must have appropriate knowledge, skills and expertise to fully understand and monitor the risk strategy and the risk appetite of the *firm*.

(2) The risk committee must advise the *management body* on the institution's overall current and future risk appetite and assist the *management body* in overseeing the implementation of that strategy by *senior management*.

(3) The risk committee must review whether prices of liabilities and assets offered to clients take fully into account the *firm's* business model and risk strategy. Where prices do not properly reflect risks in accordance with the business model and risk strategy, the risk committee must present a remedy plan to the *management body*.

[**Note**: article 76(3) of *CRD*]

7.1.18A G

7.1.18AA G A *CRR firm* which is not a *significant IFPRU firm* may combine the risk committee with the audit committee.

[**Note**: article 76(3) of *CRD*]

7.1.18B R Members of the combined risk and audit committee must have the knowledge, skills and expertise required for both committees.

[**Note**: article 76(3) of *CRD*]

7.1.19 R (1) A *CRR firm* must ensure that the *management body* in its supervisory function and, where a risk committee has been established, the risk committee have adequate access to information on the risk profile of the *firm* and, if necessary and appropriate, to the risk management function and to external expert advice.

(2) The *management body* in its supervisory function and, where one has been established, the risk committee must determine the nature, the amount, the format, and the frequency of the information on risk which it is to receive.

[**Note**: article 76(4) of *CRD*]

7.1.20 R In order to assist in the establishment of sound remuneration policies and practices, the risk committee must, without prejudice to the tasks of the remuneration committee, examine whether incentives provided by the remuneration system take into consideration risk, capital, liquidity and the likelihood and timing of earnings.

[**Note**: article 76(4) of *CRD*]

7.1.21 R (1) A *CRR firm's* risk management function (article 23 of the *MiFID Org Regulation*) must be independent from the operational functions and have sufficient authority, stature, resources and access to the *management body*.

(2) The risk management function must ensure that all material risks are identified, measured and properly reported. It must be actively involved in elaborating the *firm's* risk strategy and in all material risk management decisions and it must be able to deliver a complete view of the whole range of risks of the *firm*.

(3) A *CRR firm* must ensure that the risk management function is able to report directly to the *management body* in its supervisory function, independent from *senior management* and that it can raise concerns and warn the *management body*, where appropriate, where specific risk developments affect or may affect the *firm*, without prejudice to the responsibilities of the *management body* in its supervisory and/or managerial functions pursuant to the *CRD* and the *CRR*.

[**Note**: article 76(5) of *CRD*]

7.1.22 R The head of the risk management function must be an independent senior manager with distinct responsibility for the risk management function. Where the nature, scale and complexity of the activities of the *CRR firm* do not justify a specially appointed person, another senior person within the *firm* may fulfil that function, provided there is no conflict of interest. The head of the risk management function must not be removed without prior approval of the *management body* and must be able to have direct access to the *management body* where necessary.

[**Note**: article 76(5) of *CRD*]

7.1.23 G (1) This *guidance* is relevant to a *relevant authorised person* that has appointed a head of the risk management function.

(2) Taking account of the nature, scale and complexity of its activities, the *firm* should have appropriate procedures to ensure that the removal or any other disciplinary sanctioning of the head of the risk management function does not undermine the independence of the risk management function.

(3) It will be appropriate, in many cases, for the procedures in (2) to include that any approval for the removal of the head of the risk management function requires the approval of a majority of the *management body*, including at least a majority of its members who do not perform any executive function in the *firm*.

(4) It will also be appropriate, in many cases, for any other disciplinary sanctioning of the head of the risk management function to require the approval of a majority of the *management body*, including at least a majority of its members who do not perform any executive function in the *firm*.