PRA RULEBOOK: CRR FIRMS: INTERNAL GOVERNANCE INSTRUMENT 2015

Powers exercised

A. The Prudential Regulation Authority ("PRA") 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 137G (The PRA's general rules);
(2) section 137H (General rules about remuneration);
(3) section 137P (Control of information rules); and
(4) section 137T (General supplementary powers).

B. The rule-making powers referred to above are specified for the purpose of section 138G (2) (Rule-making instruments) of the Act.

Pre-conditions to making

C. In accordance with section 138J of the Act (Consultation by the PRA), the PRA consulted the Financial Conduct Authority. After consulting, the PRA published a draft of the proposed rules and had regard to representations made.

PRA Rulebook: CRR Firms: Internal Governance Instrument 2015

D. The PRA makes the rules in Annexes A to F to this instrument.

Part	Annex
General Organisational Requirements	A
Skills, Knowledge and Expertise	B
Compliance and Internal Audit	C
Risk Control	D
Outsourcing	E
Record Keeping	F

Commencement

E. This instrument comes into force on 2 April 2015.

Citation

F. This instrument may be cited as the PRA Rulebook: CRR Firms: Internal Governance Instrument 2015.

By order of the Board of the Prudential Regulation Authority
30 March 2015

Annex A

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

Part

GENERAL ORGANISATIONAL REQUIREMENTS

Chapter content

Links

1 APPLICATION AND DEFINITIONS

1.1 Unless otherwise stated, this Part applies to a *CRR firm*;

(1) with respect to the carrying on of the following from an establishment in the *UK*:

(a) *regulated activities*;

(b) activities that constitute *dealing in investments as principal*, disregarding the exclusion in article 15 of *Regulated Activities Order*;

(c) *ancillary activities*;

(d) in relation to *MiFID business*, *ancillary services*; and

(e) *unregulated activities* in a *prudential context*; and

(2) with respect to the carrying on of *passported activities* by it from a *branch* in another *EEA state*;

(3) in a *prudential context* with respect to activities wherever they are carried on; and

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

1.2 In this Part, the following definitions shall apply:

chief executive function

means *PRA controlled function* CF3 in the *table of PRA controlled functions,* described more fully in *SUP* 10B.6.7R of the *PRA Handbook.*

PRA controlled function

means a function, relating to the carrying on of a *regulated activity* by a *firm*, which is specified by the *PRA* (in the *table of PRA controlled functions*), under section 59 of *FSMA*.

table of PRA controlled functions

means the table of *PRA* controlled functions in *SUP* 10B.4.3R of the *PRA Handbook*.

2 GENERAL REQUIREMENTS

2.1 A *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: Art. 74(1) of the *CRD*, Art. 13(5) second paragraph of *MiFID*]

2.2 The arrangements, processes and mechanisms referred to in 2.1 must be comprehensive and proportionate to the nature, scale and complexity of the risks inherent in the business

model and of the *firm's* activities and must take into account the specific technical criteria described in 2.6, Skills, Knowledge and Expertise 3.2, Risk Control and (for a *firm* to which SYSC 19A applies), SYSC 19A of the *PRA Handbook*.

2.3 A *firm* must, taking into account the nature, scale and complexity of the business of the *firm*, and the nature and range of the financial services and activities undertaken in the course of that business establish, implement and maintain:

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

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

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

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

2.4 A *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: Art. 5(2) of the *MiFID implementing Directive*]

2.5 A *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: Art. 13(4) of *MiFID*]

2.6 A *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 those activities.

[Note: Art. 5(3) of the *MiFID implementing Directive* and Art 85(2) of the *CRD*]

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

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

2.8 A *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 2.3 to 2.7 and take appropriate measures to address any deficiencies.

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

2.9 (1) A *firm* must have in place appropriate procedures for its employees to report breaches internally through a specific, independent and autonomous channel.

(2) The channel in (1) may be provided through arrangements provided for by social partners.

[Note: Art. 71 (3) of the *CRD*]

3 PERSONS WHO EFFECTIVELY DIRECT THE BUSINESS

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

[Note: Art. 9(1) of *MiFID*, Art. 13(1) of the *CRD*]

3.2 A *firm* must ensure that its management is undertaken by at least two persons meeting the requirements laid down in 3.1.

[Note: Art. 9(4) first paragraph of *MiFID* and Art. 13(1) of the *CRD*]

4 RESPONSIBILITY OF SENIOR PERSONNEL

4.1 A *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 the *regulatory system*. 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 the *regulatory system* and take appropriate measures to address any deficiencies.

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

4.2 A *firm* must ensure that:

(1) its *senior personnel* receive on a frequent basis, and at least annually, written reports on the matters covered by Compliance and Internal Audit 2.2 to 2.4 and 3.1, and Risk Control 2.1, 2.2 and 2.4 to 2.6, indicating in particular whether the appropriate remedial measures have been taken in the event of any deficiencies; and

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

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

5 MANAGEMENT BODY

5.1 A *firm* must ensure that the *management body* defines, oversees and is accountable for the implementation of governance arrangements that ensure effective and prudent management of the *firm*, including the segregation of duties in the organisation and the prevention of conflicts of interest. The *firm* must ensure that the *management body*:

(1) has overall responsibility for the *firm*;

(2) approves and oversees implementation of the *firm's* strategic objectives, risk strategy and internal governance;

(3) ensures the integrity of the *firm's* accounting and financial reporting systems, including financial and operational controls and compliance with the *regulatory system*;

(4) oversees the process of disclosure and communications;

(5) has responsibility for providing effective oversight of *senior management*; and

(6) monitors and periodically assesses the effectiveness of the *firm's* governance arrangements and takes appropriate steps to address any deficiencies.

[Note: Art. 88(1) of the *CRD*]

5.2 A *firm* must ensure that the members of the *management body* of the *firm*:

(1) are of sufficiently good repute;

(2) possess sufficient knowledge, skills and experience to perform their duties;

(3) possess adequate collective knowledge, skills and experience to understand the *firm's* activities, including the main risks;

(4) reflect an adequately broad range of experiences;

(5) commit sufficient time to perform their functions in the *firm*; and

(6) act with honesty, integrity and independence of mind to effectively assess and challenge the decisions of *senior management* where necessary and to effectively oversee and monitor management decision-making.

[Note: Art. 91(1)-(2) and (7)-(8) of the *CRD*]

5.3 A *firm* must devote adequate human and financial resources to the induction and training of members of the *management body*.

[Note: Art. 91(3) of the *CRD*]

5.4 A *firm* must ensure that the members of the *management body* of the *firm* do not hold more directorships than is appropriate taking into account individual circumstances and the nature, scale and complexity of the *firm's* activities.

[Note: Art. 91(3) of the *CRD*]

5.5 (1) A *firm* that is significant must ensure that the members of the *management body* of the *firm* do not hold more than one of the following combinations of directorship in any organisation at the same time:

(a) one executive directorship with two non-executive directorships; and

(b) four non-executive directorships.

(2) Paragraph (1) does not apply to members of the *management body* that represent the *UK*.

[Note: Art. 91(3) of the ***CRD*]**

5.6 For the purposes of 5.4 and 5.5:

(1) directorships in organisations which do not pursue predominantly commercial objectives shall not count; and

(2) the following shall count as a single directorship:

(a) executive or non-executive directorships held within the same *group*; or

(b) executive or non-executive directorships held within:

(i) *firms* that are members of the same institutional protection scheme provided that the conditions set out in Article 113(7) of the *CRR* are fulfilled; or

(ii) *undertakings* (including non-financial entities) in which the *firm* holds a *qualifying holding*.

[Note: Art. 91(4) and (5) of the *CRD*]

5.7 A *firm* must ensure that the chairman of the *firm's management body* does not exercise simultaneously the *chief executive function* within the same *firm*, unless justified by the *firm* and authorised by the *PRA*.

[Note: Art. 88(1)(e) CRD]

5.8 A *firm* that maintains a website must explain on the website how it complies with the requirements of this Chapter.

[Note: Art. 96 of the *CRD*]

6 NOMINATION COMMITTEE

6.1 A *firm* that is significant must:

(1) establish a nomination committee composed of members of the *management body* who do not perform any executive function in the *firm*;

(2) ensure that the nomination committee is able to use any forms of resources the nomination committee deems appropriate, including external advice; and

(3) ensure that the nomination committee receives appropriate funding.

[Note: Art. 88(2) of the *CRD*]

6.2 A *firm* that has a nomination committee must ensure that the nomination committee:

(1) engage a broad set of qualities and competences when recruiting members to the *management body* and for that purpose puts in place a policy promoting diversity on the *management body*;

(2) identifies and recommends for approval, by the *management body* or by general meeting, candidates to fill *management body* vacancies, having evaluated the balance of knowledge, skills, diversity and experience of the *management body*;

(3) prepares a description of the roles and capabilities for a particular appointment, and assesses the time commitment required;

(4) decides on a target for the representation of the underrepresented gender in the *management body* and prepares a policy on how to increase the number of the underrepresented gender in the *management body* in order to meet that target;

(5) periodically, and at least annually, assesses the structure, size, composition and performance of the *management body* and makes recommendations to the *management body* with regard to any changes;

(6) periodically, and at least annually, assesses the knowledge, skills and experience of individual members of the *management body* and of the *management body* collectively, and reports this to the *management body*;

(7) periodically reviews the policy of the *management body* for selection and appointment of *senior management* and makes recommendations to the *management body*; and

(8) in performing its duties, and to the extent possible, on an ongoing basis, takes account of the need to ensure that the *management body's* decision making is not dominated by any one individual or small group of individuals in a manner that is detrimental to the interest of the *firm* as a whole.

[Note: Art. 88(2) and Art. 91(10) of the *CRD*]

6.3 A *firm* that does not have a nomination committee must engage a broad set of qualities and competences when recruiting members to the *management body*. For that purpose a *firm* that does not have a nomination committee must put in place a policy promoting diversity on the *management body*.

[Note: Art. 91(10) of the *CRD*]

6.4 A *firm* that maintains a website must explain on the website how it complies with the requirements of this Chapter.

[Note: Art. 96 of the *CRD*]

Part

GENERAL ORGANISATIONAL REQUIREMENTS

Externally defined glossary terms

Term	Definition source
EEA State	*Schedule 1 Interpretation Act 1978*
group	*s421 FSMA*
person	*Schedule 1 Interpretation Act 1978*
qualifying holding	*Art. 4(1)(36) of the CRR*
regulated activity	*s22 FSMA*

Annex B

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

Part

SKILLS, KNOWLEDGE AND EXPERTISE

Chapter content

Links

1 APPLICATION

1.1 Unless otherwise stated, this Part applies to a *CRR firm*

(1) with respect to the carrying on of the following from an establishment in the *UK*:

(a) *regulated activities*;

(b) activities that constitute *dealing in investments as principal*, disregarding the exclusion in article 15 of *Regulated Activities Order*;

(c) *ancillary activities*;

(d) in relation to *MiFID business*, *ancillary services*; and

(e) *unregulated activities* in a *prudential context*; and

(2) with respect to the carrying on of *passported activities* by it from a *branch* in another *EEA state*;

(3) in a *prudential context* with respect to activities wherever they are carried on; and

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

2 SKILLS, KNOWLEDGE AND EXPERTISE

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

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

3 SEGREGATION OF FUNCTIONS

3.1 A *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: Art. 5(1)(g) of the *MiFID implementing Directive*]

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

[Note: Art. 88 of the *CRD*]

4 AWARENESS OF PROCEDURES

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

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

5 GENERAL

5.1 The systems, internal control mechanisms and arrangements established by a *firm* in accordance with this Part must take into account the nature, scale and complexity of its

business and the nature and range of financial services and activities undertaken in the course of that business.

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

5.2 A *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 Part, and take appropriate measures to address any deficiencies.

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

Part

SKILLS, KNOWLEDGE AND EXPERTISE

Externally defined glossary terms

Term	Definition source
EEA State	*Schedule 1 Interpretation Act 1978*
group	*s421 FSMA*
person	*Schedule 1 Interpretation Act 1978*
regulated activity	*s22 FSMA*

Annex C

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

Part

COMPLIANCE AND INTERNAL AUDIT

Chapter content

Links

1 APPLICATION AND DEFINITIONS

1.1 Unless otherwise stated, this Part applies to a *CRR firm*

(1) with respect to the carrying on of the following from an establishment in the *UK*:

(a) *regulated activities*;

(b) activities that constitute *dealing in investments as principal*, disregarding the exclusion in article 15 of *Regulated Activities Order*;

(c) *ancillary activities*;

(d) in relation to *MiFID business*, *ancillary services*; and

(e) *unregulated activities* in a *prudential context*; and

(2) with respect to the carrying on of *passported activities* by it from a *branch* in another *EEA state*;

(3) in a *prudential context* with respect to activities wherever they are carried on; and

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

1.2 In this Part, the following definitions shall apply:

competent authority

means the authority, designated by each *EEA State* in accordance with Article 48 of *MiFID*, unless otherwise specified in *MiFID.*

[Note: Art. 4(1)(22) of *MiFID*]

host Member State

has the meaning given in Article 4(1)(21) of *MiFID*.

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

2 COMPLIANCE

2.1 A *firm* must establish, implement and maintain adequate policies and procedures sufficient to ensure compliance of the firm including its managers, *employees* and *appointed representatives* (or where applicable, *tied agents*) with its obligations under the *regulatory system* and for countering the risk that the firm might be used to further *financial crime*.

[Note: Art. 13(2) of *MiFID*]

2.2 A *firm* must, taking into account the nature, scale and complexity of its business, and the nature and range of financial 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 *PRA* to exercise its powers effectively under the *regulatory*

system and to enable any other *competent authority* to exercise its powers effectively under *MiFID*.

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

2.3 A *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 2.2 and the actions taken to address any deficiencies in the *firm's* compliance with its obligations; and

(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: Art. 6(2) of the *MiFID implementing Directive*]

2.4 In order to enable the compliance function to discharge its responsibilities properly and independently, a *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 General Organisation Requirements 4.2;

(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: Art. 6(3) first paragraph of the *MiFID implementing Directive*]

2.5 A *firm* need not comply with 2.4(3) or (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 financial services and activities, the requirements under those rules are not proportionate and that its compliance function continues to be effective.

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

2.6 (1) This rule applies to a *firm* conducting *investment services and activities* from a *branch* in another *EEA State*.

(2) References to the *regulatory system* in 2.1, 2.2 and 2.3 apply in respect of a *firm's branch* as if *regulatory system* includes a *host Member State's* requirements under *MiFID* and the *MiFID implementing Directive* which are applicable to the *investment services and activities* conducted from the *firm's branch*.

[Note: Art. 13(2) of *MiFID*]

3 INTERNAL AUDIT

3.1 A *firm* must, where appropriate and proportionate in view of the nature, scale and complexity of its business and the nature and range of its financial 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; and

(4) to report in relation to internal audit matters in accordance with General Organisational Requirements 4.2.

[Note: Art. 8 of the *MiFID implementing Directive*]

Part

COMPLIANCE AND INTERNAL AUDIT

Externally defined glossary terms

Term	Definition source
EEA State	*Schedule 1 Interpretation Act 1978*
group	*s421 FSMA*
financial crime	*s1H FSMA*
person	*Schedule 1 Interpretation Act 1978*
regulated activity	*s22 FSMA*

Annex D

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

Part

RISK CONTROL

Chapter content

Links

1 APPLICATION

1.1 Unless otherwise stated, this Part applies to a *CRR firm*

(1) with respect to the carrying on of the following from an establishment in the *UK*:

(a) *regulated activities*;

(b) activities that constitute *dealing in investments as principal*, disregarding the exclusion in article 15 of *Regulated Activities Order*;

(c) *ancillary activities*;

(d) in relation to *MiFID business*, *ancillary services*; and

(e) *unregulated activities* in a *prudential context*; and

(2) with respect to the carrying on of *passported activities* by it from a *branch* in another *EEA state*;

(3) in a *prudential context* with respect to activities wherever they are carried on; and

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

2 RISK CONTROL

2.1 A *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: Art. 7(1)(a) of the *MiFID implementing Directive*, Art. 13(5) second paragraph of *MiFID*]

2.2 A *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: Art. 7(1)(b) of the *MiFID implementing Directive*]

2.3 The *management body* of a *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: Art. 76(1) of the CRD]

2.4 A *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 2.2;

(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: Art. 7(1)(c) of the *MiFID implementing Directive*]

2.5 A *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 2.1 to 2.4; and

(2) provision of reports and advice to *senior personnel* in accordance with General Organisational Requirements 4.2.

[Note: Art. 7(2) first paragraph of the *MiFID implementing Directive*]

2.6 Where a *firm* is not required under 2.5 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 2.1 to 2.4 satisfy the requirements of those rules and are consistently effective.

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

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

(2) The *management body* of a *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 *CRR* as well as in the valuation of assets, the use of external ratings and internal models related to those risks.

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

[Note: Art. 76(2) of the *CRD*]

3 RISK COMMITTEE

3.1 (1) A *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: Art. 76(3) of the *CRD*]

3.2 (1) A *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: Art. 76(4) of the *CRD*]

3.3 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: Art. 76(4) of the *CRD*]

3.4 (1) A *firm's* risk management function (2.5) 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 *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: Art. 76(5) of the *CRD*]

3.5 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 *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: Art. 76(5) of *the CRD*]

Part

RISK CONTROL

Externally defined glossary terms

Term	Definition source
EEA State	*Schedule 1 Interpretation Act 1978*
group	*s421 FSMA*
person	*Schedule 1 Interpretation Act 1978*
regulated activity	*s22 FSMA*

Annex E

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

Part

OUTSOURCING

Chapter content

Links

1 APPLICATION AND DEFINITIONS

1.1 Unless otherwise stated, this Part applies to a *CRR firm*

(1) with respect to the carrying on of the following from an establishment in the *UK*:

(a) *regulated activities*;

(b) activities that constitute *dealing in investments as principal*, disregarding the exclusion in article 15 of *Regulated Activities Order*;

(c) *ancillary activities*;

(d) in relation to *MiFID business*, *ancillary services*; and

(e) *unregulated activities* in a *prudential context*; and

(2) with respect to the carrying on of *passported activities* by it from a *branch* in another *EEA state*;

(3) in a *prudential context* with respect to activities wherever they are carried on; and

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

1.2 In this Part, the following definitions shall apply:

authorisation

means *authorisation* as an *authorised person* for the purposes of *FSMA*.

control

means control as defined in Article 1 of the Seventh Council Directive 83/349/EEC (The Seventh Company Law Directive).

listed activities

means an activity listed in Annex 1 to the *CRD.*

relevant services and activities

means *regulated activities, listed activities* or *ancillary services*.

2 OUTSOURCING

2.1 A *firm* must:

(1) when relying on a third party for the performance of operational functions which are critical for the performance of *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 *outsourcing* 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 *PRA* 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: Art. 13(5) first paragraph of *MiFID*]

2.2 For the purposes of this Part 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 *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: Art. 13(1) of the *MiFID implementing Directive*]

2.3 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 Part:

(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; and

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

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

2.4 If a *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: Art. 14(1) of the *MiFID implementing Directive*]

2.5 A *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: Art. 14(2) first paragraph of the *MiFID implementing Directive*]

2.6 A *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 to manage the risks associated with the *outsourcing*, 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 *PRA* and any other relevant *competent authority* in connection with the *outsourced* activities;

(9) the *firm*, its auditors, the *PRA* 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 *PRA* 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: Art. 14(2) second paragraph of the *MiFID implementing Directive*]

2.7 A *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: Art. 14(3) of the *MiFID implementing Directive*]

2.8 If a *firm* and the service provider are members of the same *group*, the *firm* may, for the purpose of complying with 2.5 to 2.9, take into account the extent to which the *firm controls* the service provider or has the ability to influence its actions.

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

2.9 A *firm* must make available on request to the *PRA* and any other relevant *competent authority* all information necessary to enable the *PRA* 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: Art. 14(5) of the *MiFID implementing Directive*]

Part

OUTSOURCING

Externally defined glossary terms

Term	Definition source
authorised person	*Schedule 1 Interpretation Act 1978*
EEA State	*Schedule 1 Interpretation Act 1978*
group	*s421 FSMA*
person	*Schedule 1 Interpretation Act 1978*
regulated activity	*s22 FSMA*

Annex F

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

Part

RECORD KEEPING

Chapter content

Links

1 APPLICATION

1.1 Unless otherwise stated, this Part applies to a *CRR firm*

(1) with respect to the carrying on of the following from an establishment in the *UK*:

(a) *regulated activities*;

(b) activities that constitute *dealing in investments as principal*, disregarding the exclusion in article 15 of *Regulated Activities Order*;

(c) *ancillary activities*;

(d) in relation to *MiFID business*, *ancillary services*; and

(e) *unregulated activities* in a *prudential context*; and

unless another applicable rule which is relevant to the activity has a wider territorial scope, in which case this Part applies with that wider scope in relation to the activity described in that rule

(2) with respect to the carrying on of *passported activities* by it from a *branch* in another *EEA state*;

(3) in a *prudential context* with respect to activities wherever they are carried on; and

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

2 RECORD KEEPING

2.1 A *firm* must arrange for orderly records to be kept of its business and internal organisation, including all services and transactions undertaken by it, which must be sufficient to enable the *PRA* or any other relevant competent authority under *MiFID* to monitor the *firm's* compliance with the requirements under the *regulatory system*, and in particular to ascertain that the *firm* has complied with all obligations with respect to *clients*.

[Note: Art. 13(6) of *MiFID*, and Art. 5(1)(f) of the *MiFID implementing Directive*]

2.2 A *firm* must retain all records kept by it under this Part in relation to its *MiFID business* for a period of at least five years.

[Note: Art. 51 (1) of the *MiFID implementing Directive*]

2.3 In relation to its *MiFID business*, a *firm* must retain records in a medium that allows the storage of information in a way accessible for future reference by the *PRA* or any other relevant *competent authority* under *MiFID*, and so that the following conditions are met:

(1) the *PRA* or any other relevant *competent authority* under *MiFID* must be able to access them readily and to reconstitute each key stage of the processing of each transaction;

(2) it must be possible for any corrections or other amendments, and the contents of the records prior to such corrections and amendments, to be easily ascertained; and

(3) it must not be possible for the records otherwise to be manipulated or altered.

[Note: Art. 51(2) of the *MiFID implementing Directive*]

RECORD KEEPING

Externally defined glossary terms

Term	Definition source
EEA State	*Schedule 1 Interpretation Act 1978*
group	*s421 FSMA*
regulated activity	*s22 FSMA*