Chapter 2

Senior management arrangements, systems and controls

2.2 General provisions

Appropriate systems and controls

2.2.1 G ■ SYSC 4.1.1 R requires every *firm*, including a *credit union*, to 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.

2.2.2 G For *credit unions*, the arrangements, processes and mechanisms referred to in ■ SYSC 4.1.1 R should be comprehensive and proportionate to the nature, scale, and complexity of the risks inherent in the business model and of the *credit union's* activities. That is the effect of ■ SYSC 4.1.2 R and ■ SYSC 4.1.2A G.

2.2.3 G A *credit union's* systems and controls should be proportionate to the nature, scale and complexity of the activities it undertakes. For instance, a small *credit union* will not usually be expected to have the same systems and controls as a large one, and a *credit union* offering only basic savings accounts and loans will not be expected to have the same systems and controls as one offering a wider range of services or more complicated products.

Business plan

2.2.4 R A *credit union* must establish, maintain and implement an up-to-date business plan approved by its *governing body*.

2.2.5 G *Guidance* on business planning is given in ■ CREDS 2.2.51 G to ■ CREDS 2.2.58 G.

Policies and procedures manual

2.2.6 R A *credit union* must establish, maintain, and implement an up-to-date and fully documented policies and procedures manual.

2.2.7 G *Guidance* on documentation of policies and procedures is given in ■ CREDS 2.2.59 G to ■ CREDS 2.2.61 G.

System of control

2.2.8 R A *credit union* must establish, maintain and implement a fully documented system of control.

2.2.9 G *Guidance* on the documentation of systems of control is given in ■ CREDS 2.2.20 G to ■ CREDS 2.2.23 G.

Internal audit function

2.2.10 E [deleted]

2.2.10A E If a *credit union* does not have an internal audit function, this may be relied on as tending to establish contravention of ■ SYSC 4.1.1R (see ■ CREDS 2.2.1G).

2.2.11 G (1) The term 'internal audit function' in ■ CREDS 2.2.10 E refers to the generally understood concept of internal audit within a *firm*, in other words the function of assessing adherence to and the effectiveness of internal systems and controls, procedures and policies.

(2) *Guidance* on internal audit is given in ■ CREDS 2.2.40 G to ■ CREDS 2.2.50 G.

Segregation of duties

2.2.12 G A *credit union* should ensure appropriate segregation of duties in order to minimise the risk of *financial crime* or contravention of requirements and standards under the *regulatory system*.

2.2.13 G *Guidance* on segregation of duties is given in ■ CREDS 2.2.18 G and ■ CREDS 2.2.19 G.

Governing body

2.2.14 G Under section 4(1) of, and Schedule 1 to, the Credit Unions Act 1979 or article 8(1) of, and Schedule 1 to, the Credit Unions (Northern Ireland) Order 1985, as appropriate, a *credit union* is required to have a committee of management, managers or other officers, or a board of directors (a *governing body*). This body should be competent to control the affairs of a *credit union*, and have an appropriate range of skills and experience relevant to the activities carried on by the *credit union*.

2.2.15 G In accordance with *rule* SC 2 in ■ COCON 2.2.1R, it is the responsibility of each individual member of the *governing body* who is a *senior conduct rules staff member* to understand, and ensure that the *credit union* complies with, the requirements of all the relevant Acts, secondary legislation and *rules*.

2.2.16 G (1) The *credit union's governing body* has responsibility for ensuring that the *credit union* complies with the requirements of ■ SYSC 4.1.1 R (see ■ CREDS 2.2.1 G and ■ CREDS 2.2.2 G). So, the *governing body* has overall responsibility for:

(a) establishing objectives and formulating a business plan;

(b) monitoring the financial position of the *credit union*;

(c) determining and documenting policies and procedures;

(d) directing and coordinating the work of all *employees* and volunteers, and ensuring that they are capable and properly trained;

(e) maintaining adequate reserves;

(f) making provision for bad and doubtful debts;

(g) recommending a dividend on shares to members subject to the *credit union's* financial position;

(h) ensuring that the *credit union* complies with all statutory and regulatory requirements; and

(i) ensuring that the *credit union* complies with the requirements of its registered rules.

(2) [deleted]

2.2.17 G The *governing body* should meet at least monthly.

Organisation

2.2.18 G ■ CREDS 2.2.12 G states that all *credit unions* should ensure appropriate segregation of duties. Duties should be segregated to prevent one individual from initiating, controlling, and processing a transaction (for example, both the approval and the payment of an invoice).

2.2.19 G Responsibilities of connected *persons* (for example, relatives and other close relationships) should be kept entirely separate. They should not hold key posts at the same time as each other. Where this is unavoidable, a *credit union* should have a written policy for ensuring complete segregation of duties and responsibilities.

Documentation of systems of control

2.2.20 G ■ CREDS 2.2.8 R requires a *credit union's* system of control to be fully documented. The documentation helps the *governing body* to assess if systems are maintained and controls are operating effectively. It also helps those reviewing the systems to verify that the controls in place are those that have been authorised, and that they are adequate for their purpose.

2.2.21 G (1) The *governing body* should decide what form this documentation should take, but the *governing body* should have in mind the following points.

(a) Documents should be comprehensive: they should cover all material aspects of the operations of the *credit union*.

(b) Documents should be integrated: separate elements of the system should be cross-referred so that the system can be viewed as a whole.

(c) Documents should identify risks and the controls established to manage those risks. The controls should be identified and their purpose defined so that their effectiveness can be evaluated.

(d) There should be named *persons* or posts for each control function and alternatives in case of absence.

(e) Documents should state how the operation of the control is evidenced. Evidence might include signatures, records and registers. Documents should also state for how long that evidence is to be retained, taking account of ■ SYSC 9.1.

(f) Documents should be unambiguous. Instructions should be clear and precise, avoiding expressions such as "normally" and "if possible".

(g) Documents should be practical and easy to consult and use when operating and reviewing systems.

(h) Documents should be up to date. There should be an accurate description of the function that the control is to address. When changes are made to the function, the appropriate systems of control need to be updated and documented at the same time.

(2) The *governing body* should, from time to time, seek confirmation that the systems of control are being complied with.

2.2.22 G Documentation should not be restricted to "lower level" controls applied in processing transactions, but should also cover "high level" controls including:

(1) identifying those powers to be exercised only by the *governing body*, and the powers delegated to others;

(2) the purpose, composition and reporting lines of sub-committees, and *senior managers* to whom responsibilities are delegated;

(3) the specific roles and responsibilities of individual *officers*;

(4) the timing, form and purpose of meetings of the *governing body* and sub-committees, and the way in which policies and decisions are recorded and their implementation monitored.

2.2.23 G The documentation of IT controls should be integrated within the overall documentation of a *credit union's* system of control.

Accounting records and systems

2.2.24 G ■ SYSC 9.1.1 R requires that a *credit union* takes reasonable care to make and retain adequate records of all matters governed by the *Act* or the *CCA*, secondary legislation under the *Act* or the *CCA*, or *rules* (including accounting records). These records should be capable of being reproduced in the English language and on paper.

2.2.25 G A *credit union* should have appropriate systems in place to fulfil its obligations with respect to adequacy, access, periods of retention, and security of records.

2.2.26 G The main reasons why a *credit union* should maintain adequate accounting and other records are:

(1) to provide the *governing body* with adequate financial and other information to enable it to conduct its business in a prudent manner on a day-to-day basis;

(2) to safeguard the assets of the *credit union* and the interests of members and *persons* too young to be members;

(3) to assist *officers* of the *credit union* to fulfil their regulatory and statutory duties in relation to the preparation of annual accounts;

(4) to provide the *governing body* with sufficient timely and accurate information to assist them to submit the information required or requested by the*FCA*.

2.2.27 G [deleted]

2.2.28 G [deleted]

2.2.28A R The *governing body* must satisfy itself that the accounting and other records are maintained in a complete, integrated and orderly manner in order to disclose, with reasonable accuracy and promptness, the state of the business at any time.

The compliance function

2.2.29 G (1) Depending on the nature, scale and complexity of its business, it may be appropriate for a *credit union* to have a separate compliance function.

(2) The organisation and responsibilities of a compliance function should be documented.

(3) A compliance function should be staffed by an appropriate number of competent staff who are sufficiently independent to perform their duties objectively. It should be adequately resourced and should have unrestricted access to the *credit union's* relevant records as well as ultimate recourse to its *governing body*.

2.2.30 G *Guidance* on compliance is located in ■ SYSC 6.1.3 R.

[**Note**: As explained in ■ SYSC 1 Annex 1.3.3G, ■ SYSC 6.1.3 R is to be read as *guidance* rather than as a *rule*, and as if "should" appeared in that provision instead of "must".]

2.2.31 G Some important compliance issues include:

(1) insurance against fraud and dishonesty;

(2) arrangements for the prevention, detection and reporting of *money laundering*;

(3) establishing and maintaining a satisfactory system of control;

(4) keeping proper books of account;

(5) computation and application of profits;

(6) investment of surplus funds;

(7) capital requirements;

(8) liquidity requirements;

(9) limits on shares and loans;

(10) maintenance of membership records;

(11) submission of financial reports to the regulator;

(12) [deleted]

(13) payment of regulatory fees.

Management information

2.2.32 G *Guidance* on management information is located in ■ SYSC 7.1.4 R.

[**Note**: As explained in ■ SYSC 1 Annex 1.3.3G, ■ SYSC 7.1.4 R is to be read as *guidance* rather than as a *rule*, and as if "should" appeared in that provision instead of "must".]

2.2.33 G [deleted]

2.2.33A R A *credit union* must maintain information systems to enable the *governing body* to direct and control the *credit union's* business effectively, and to provide the information required by the *FCA*.

2.2.34 G [deleted]

2.2.34A R The *governing body* must be satisfied that:

(1) the information available is sufficiently comprehensive for the proper assessment of the potential risks for the *credit union*, and in order to determine its need for capital and liquidity;

(2) the information available is sufficiently comprehensive to provide a clear statement of the performance and financial position of the *credit union*;

(3) management information reports are prepared with sufficient frequency;

(4) sufficient attention is focused on key factors affecting income and expenditure and that appropriate performance indicators are employed; and

(5) actual performance is compared with planned and previous performance.

2.2.35 G In forming a view on whether the management information system is sufficiently comprehensive, the *governing body* should consider whether, where relevant, the substance of reports provides a clear statement of loans, arrears and provisions. These matters should be compared against limits, ratios and other parameters set by the *governing body*, as well as regulatory requirements.

2.2.36 G [deleted]

2.2.37 G [deleted]

Personnel

2.2.38 G *Guidance* on *employees* and agents is located in ■ SYSC 5.1.2 G.

2.2.39 G A *credit union* should identify present and future staffing requirements (including volunteers and paid staff) and make appropriate plans for their recruitment and training.

Internal Audit

2.2.40 G ■ CREDS 2.2.10AE states that if a *credit union* does not have an audit function, this may be relied on as tending to establish contravention of ■ SYSC 4.1.1R.

2.2.41 G *Guidance* on internal audit and audit committees (otherwise known as the supervisory committee) is located in ■ SYSC 6 and ■ SYSC 4.1.11 G.

2.2.42 G Depending upon the scale and nature of the *credit union's* activities, it may be appropriate for the audit committee to delegate the task of monitoring the effectiveness and appropriateness of its systems and controls to an *employee* or other third party.

2.2.43 G The purposes of an internal audit are:

(1) to ensure that the policies and procedures of the *credit union* are followed;

(2) to provide the *governing body* with a continuous appraisal of the overall effectiveness of the control systems, including proposed changes;

(3) to recommend improvements where desirable or necessary;

(4) to determine whether the *internal controls* established by the *governing body* are being maintained properly and operated as laid down in the policy, and comply with relevant Acts, secondary legislation, *rules*, policies and procedures;

(5) to ensure that accounting records are prepared promptly and accurately, and that they are in order;

(6) to assess whether financial and operating information supplied to the *governing body* is accurate, pertinent, timely, and complete.

2.2.44 G The internal audit function (see ■ CREDS 2.2.11G) should develop an audit plan, covering all aspects of the *credit union's* business. The audit plan should identify the scope and frequency of work to be carried out in each area. Areas identified as higher risk should be covered more frequently. However, over a set timeframe (likely to be one year) all areas should be covered. Care should be taken to avoid obvious patterns in assessing the different areas of the *credit union's* business, so that the audit plan produces a representative snapshot of the operation and effectiveness of the credit union's internal systems and controls, procedures and policies.

2.2.45 G The internal audit work programme should include items such as:

(1) verification of cash (counting and reconciliation) without prior notification;

(2) bank reconciliation (checking records against *bank* statements);

(3) verification of passbooks or account statements;

(4) checking for compliance with policies and procedures;

(5) checking for compliance with relevant Acts, secondary legislation and *rules*;

(6) checking minutes and reports of the *governing body* and other sub-committees for compliance, and assessing regularity and completeness;

(7) checking loan applications;

(8) verification of the *credit union's* assets and *investments*.

2.2.46 G The key elements of a satisfactory system of internal audit include the following:

(1) Terms of reference. These should be specified with precision and include, amongst other things, scope and objectives of the audit committee and the internal audit function (see ■ CREDS 2.2.11G), access to records, powers to obtain information and explanations for *officers*, and reporting requirements. These should be approved by the *governing body*.

(2) Risk analysis. Key risks in each area of the *credit union's* business should be identified. The adequacy of the specific controls put in place to address those risks should be assessed.

(3) Internal audit plan. This should be developed on the basis of the risk analysis.

(4) Detailed programmes. These should be based on the internal audit plan, together with the controls and their objectives specified in the control documentation. Each programme should be comprehensive, specifying the frequency with which the various parts of the programme are to be carried out and how the work is to be performed.

(5) Working papers. These should be maintained to evidence who performed the work, how it was controlled and supervised, and to record the conclusions reached. They should be cross referenced to reports made and action taken.

(6) System of reporting. Formal reports should be submitted at the completion of each aspect of programmed work, stating the areas covered together with any recommendations and conclusions reached.

2.2.47 G The internal audit function (see ■ CREDS 2.2.11 G) should be independent of all of the functions it inspects.

2.2.48 G The *governing body* should be satisfied that the status and reporting relationship of the chairman of the audit committee is sufficient to maintain the independence and objectivity of the function.

2.2.49 G The qualifications, experience and training of individuals performing the internal audit function (see ■ CREDS 2.2.11 G) should be adequate in relation to its objectives.

2.2.50 G The *governing body* should be satisfied that the internal audit function (see ■ CREDS 2.2.11 G) is being properly carried out. In order to review the overall effectiveness of the internal audit function it should consider the following:

(1) the adequacy and scope of planning;

(2) the adequacy and scope of work performed in relation to the plans and programmes;

(3) the regularity and level of reporting on matters arising from the inspections;

(4) the disposal of points and recommendations raised, and reasons for the rejection of any major points;

(5) a review of the overall effectiveness of the internal audit function.

Business planning

2.2.51 G ■ CREDS 2.2.4 R requires that a *credit union* maintains a current business plan.

2.2.52 G [deleted]

2.2.53 G *Guidance* on business strategy is located in ■ SYSC 6.1.2 R and ■ SYSC 7.1.2 R.

[**Note**: As explained in ■ SYSC 1 Annex 1.3.3G, ■ SYSC 6.1.2 R and ■ SYSC 7.1.2 R are to be read as *guidance* rather than as *rules*, and as if "should" appeared in those provisions instead of "must".]

2.2.54 G The *governing body* should have a satisfactory planning system to provide a framework for growth and development of the *credit union*, and to enable it to identify, measure, manage and control risks of regulatory concern.

2.2.55 G The business plan should cover a period of three years from the current financial year, in other words the remainder of the current financial year and the two following financial years.

2.2.56 G The planning system should be defined clearly, documented appropriately, and planning related tasks and decision-making responsibilities allocated clearly within the *credit union*.

2.2.57 G The conclusions, recommendations, projections and assumptions set out in the business plan should be supported by analysis, based on adequate data, and properly documented for comparison with actuals.

2.2.58 G The *governing body* should consider the range of possible outcomes in relation to various risks. These risks are increased when a *credit union* provides ancillary services such as issuing and administering means of payment and money transmission, which result, in particular, in higher liquidity and operational risks.

Documentation of policies and procedures

2.2.59 G ■ CREDS 2.2.6 R requires that a *credit union* maintains a manual of its policies and procedures.

2.2.60 G [deleted]

2.2.61 G The policy and procedures manual should cover all aspects of the *credit union's* operations, including matters such as:

(1) cash handling and disbursements;

(2) collection procedures;

(3) lending, (see ■ CREDS 7.1 to ■ CREDS 7.2);

(4) arrears management (see ■ CREDS 7.2.9 G to ■ CREDS 7.2.10 G);

(5) provisioning;

(6) liquidity management;

(7) financial risk management;

(8) *money laundering* prevention (see ■ SYSC 6.3);

(9) internal audit (see ■ CREDS 2.2.40 G to ■ CREDS 2.2.50 G);

(10) information technology (see ■ CREDS 2.2.23 G);

(11) business continuity, otherwise known as disaster recovery (see ■ CREDS 2.2.62 G to ■ CREDS 2.2.64 G);

(12) marketing;

(13) training;

(14) connected *persons* and managing conflicts of interest (see ■ CREDS 2.2.19 G);

(15) *complaints* handling (see ■ DISP 1).

Business continuity

2.2.62 G *Guidance* on business continuity is located in ■ SYSC 4.1.6R to ■ SYSC 4.1.8 G.

[**Note**: As explained in ■ SYSC 1 Annex 1.3.3G, ■ SYSC 4.1.6R is to be read as *guidance* rather than as a *rule*, and as if "should" appeared in that provision instead of "must".]

2.2.63 G A *credit union* should put in place contingency arrangements to ensure that it could continue to operate and meet its regulatory requirements in the event of an unforeseen interruption that may otherwise prevent the *credit union* from operating normally (for example, if there was a complete failure of IT systems or if the premises were destroyed by fire).

2.2.64 G Business continuity arrangements should be reviewed and tested regularly in order to ensure their effectiveness.

Governance and senior management arrangements: general

2.2.65 G (1) ■ SYSC 4.5, ■ SYSC 4.7 and ■ SYSC 4.9 have a number of requirements about the governance and senior management arrangements of *relevant authorised persons*.

(2) A *credit union* is a type of *relevant authorised person*.

(3) ■ SYSC 4.5, ■ SYSC 4.7 and ■ SYSC 4.9 are summarised in ■ CREDS 2.2.66G to ■ CREDS 2.2.70G.

(4) The *PRA's* requirements about the subjects dealt with in ■ SYSC 4.5, ■ SYSC 4.7 and ■ SYSC 4.9 are set out in its Rulebook. *CREDS* does not summarise them.

Governance and senior management arrangements: responsibilities map

2.2.66 G (1) ■ SYSC 4.5 says that a *relevant authorised person*, including a *credit union*, should, at all times, have a comprehensive and up-to-date

document that describes its management and governance arrangements. This is called the *management responsibilities map*.

(2) ■ SYSC 4.5.13G has *guidance* on *management responsibilities maps* for small *firms*, which is likely to be of particular relevance to *credit unions*.

Governance and senior management arrangements: allocation of senior management responsibilities

2.2.67 G ■ SYSC 4.7 says that a *relevant authorised person*, including a *credit union*, should:

(1) allocate a number of specified management responsibilities (called *FCA-prescribed senior management responsibilities*) to one or more of its *SMF managers*; and

(2) ensure that, at all times, one or more of its *SMF managers* have overall responsibility for each of the activities, business areas and management functions of the *firm*.

2.2.68 G ■ CREDS 8.3 explains what an *SMF manager* is.

2.2.69 G (1) The list of *FCA-prescribed senior management responsibilities* that a *credit union* should allocate is simpler than for most other *relevant authorised persons*.

(2) ■ SYSC 4.7.7R sets out a list of *FCA-prescribed senior management responsibilities*, including the ones that apply to *credit unions*.

Governance and senior management arrangements: handover procedures

2.2.70 G ■ SYSC 4.9 contains material about handover arrangements when an *SMF manager* (or their supervisor) takes up or leaves their job.

Certification regime

2.2.71 G Under section 63E(1) of the *Act*, a *relevant authorised person* (including a *credit union*) should take reasonable care to ensure that no employee of the *firm* performs an *FCA-specified significant-harm function* under an arrangement entered into by the *firm* in relation to the carrying on by that *firm* of a *regulated activity*, unless the employee has a valid certificate issued by that *firm* to perform the function to which the certificate relates. The definition of employee for these purposes goes beyond a conventional employee and is explained in more detail in ■ SYSC 5.2.21G. It includes volunteers or unpaid staff.

2.2.72 G ■ SYSC 5.2 gives details about the certification requirement described in ■ CREDS 2.2.71G and sets out *rules* and *guidance* about it, including a list of *FCA-specified significant-harm functions*.

2.2.73 G

(1) Section 63E(1) of the *Act* also applies to functions specified by the *PRA*.

(2) The *PRA's* certification regime (including the functions referred to in (1)) is described in its Rulebook. It is not summarised in *CREDS*.