OPERATIONAL RISK

Contents

Version History

Version	Date	Amendments
0.1	July 2013	Initial Version.
1.0	September 2013	Amended wording at Section 1.3.2 to clarify the information to be considered in assessment of operational loss.
1.1	December 2014	Amended text in section 186(3) to reflect amendment made by section 5(2) and Sch. 3, Part 2, Item 7 of the Central Bank (Supervision and Enforcement) Act 2013.
1.2	November 2015	Inserted regulations in Section 5.2.
1.3	January 2016	Updated regulations in Section 5.2.

1. Operational Risk

1.1 Legislation

Section 76E – Operational risk*

(1) In this Act 'operational risk', in relation to a credit union, means the risk of loss (financial or otherwise) resulting from—

(a) inadequate or failed internal processes or systems of the credit union,

(b) any failure by persons connected with the credit union,

(c) legal risk (including exposure to fines, penalties or damages as well as associated legal costs), or

(d) external events,

but does not include reputational risk.

(2) A credit union shall identify the operational risks it is exposed to, or is likely to be exposed to, and provide for the management and mitigation of those risks in the credit union's risk management system as provided for by section 76B.

Section 47 – Insurance against fraud of officers etc.

(1) ‡ A credit union shall at all times maintain in force, in respect of each financial year, a policy of insurance which complies with any prescribed requirements and which insures the credit union in respect of loss suffered or liability incurred by reason of the fraud or other dishonesty of its officers.

1.2 Guidance

The management and mitigation of operational risk should be fully integrated in a credit union's risk management system. As set out in the Chapter on "Risk Management and Compliance", a risk management system as required under section 76B of the 1997 Act should include the following at a minimum:

- a risk management policy;
- a risk management process;
- a risk register;
- systems and controls; and
- a review by the board of directors.

In addition to the guidance on the above set out in the Chapter on "Risk Management and Compliance", consideration should be given to the guidance set out below in respect of operational risk.

1.3 Risk management process

1.3.1 Identification of operational risk

Operational risk is inherent in all activities, processes and systems of a credit union. The risk management officer should identify the types of operational risk that the credit union is exposed to including the risk of loss resulting from the following at a minimum:

- lack of adequate security of credit union officers, assets and systems including security of information systems;
- processes and systems failures including transaction processing failures and information systems failures;
- physical damage to officers, assets and systems;
- inaccurate or inadequate management information and/or records;
- human errors or failures including failures arising from fraud; dishonesty; lack of resources, skills, training, policies, procedures, delegations; or poor management;
- failure to meet legal, contractual and other obligations including internal operational targets;
- failure to have adequate insurance policies in place or failure to review or renew them;
- material interruptions to the business of the credit union;
- outsourcing, including the adequacy of resources and expertise of the service provider;
- changes to credit union products, services, activities or operations, including those undertaken by third parties; and

- the current business operating environment including the legal, economic and regulatory climate.

1.3.2 Assessment and measurement of operational risk

In assessing operational risks, credit unions should consider the following at a minimum:

- actual operational risk losses that occurred or losses that could have occurred but were avoided;
- risk indicators such as member complaints, processing volumes, officer turnover, large number of unreconciled items, process and systems failures;
- changes in the business operating environment;
- any publically available information on operational losses or information available from other credit unions on operational problems/circumstances incurred; and
- the outcome of independent reports and evaluations such as any reports made by the auditor, asset reviews, operational reviews, internal audit reports and inspection reports.

1.3.3 Management of operational risk

The board of directors of a credit union should ensure that systems and controls are put in place to ensure operational risks are managed and mitigated. This should cover the following at a minimum:

a) in respect of the risk of loss resulting from failed internal processes and systems, ensuring that -

- adequate systems and controls, including approval processes, are in place to plan and manage changes to the operations or activities of the credit union;
- there is adequate investment in appropriate and secure information systems;
- information systems are effective and produce accurate, reliable, consistent, timely and comprehensive management information;
- there is regular verification and reconciliation of transactions and accounts;
- records are accurate, accessible and secure in accordance with the Section of this Chapter on “Records Management”; and
- systems and controls are implemented to rectify processes and systems failures;

b) in respect of the risk of loss from any failure by persons connected with the credit union, ensuring that -

- adequate segregation of duties and clear organisational and reporting structures are in place, including defined and prudent levels of decision-making authority and approval authority to ensure no one individual has responsibility for all stages of processes within the credit union (e.g. loan application, approval and drawdown);

- there is a strong operational risk management culture in the credit union and that all officers are capable of performing, and are aware of, their operational risk management responsibilities through appropriate training and supervision of officers;
- adequate resources are in place including succession plans in accordance with the Chapter on "Governance" taking account of the nature, scale, complexity and risk profile of the credit union;
- the remuneration policy is appropriate in accordance with the Chapter on "Governance";
- the standard of conduct and ethical behaviour of officers is in accordance with the Chapter on "Governance" and is communicated to all officers of the credit union;
- the performance of the manager and employees and voluntary assistants of the credit union are reviewed on an ongoing basis, as required under section 55(1) of the 1997 Act;
- systems and controls are in place to mitigate the risk of fraud and dishonesty by officers including appropriate disciplinary policies and procedures; and
- the credit union is insured against loss suffered or liability incurred by reason of the fraud or other dishonesty of its officers, as required under section 47 of the 1997 Act;

c) in respect of the risk of loss resulting from legal risk, ensuring that -

- systems and controls are in place to minimise the threat of criminal activity from both within and outside the credit union including fraud, money laundering and terrorist financing;
- the compliance officer carries out its functions in accordance with section 76D of the 1997 Act[1] to ensure that the credit union complies with all statutory and regulatory requirements and guidance;
- policies and procedures are communicated throughout the credit union; and
- weaknesses identified by the internal audit function in the effectiveness of the compliance programme are rectified in a timely manner;

d) in respect of the risk of loss resulting from external events, ensuring that -

- business continuity plans are in place, communicated to officers and tested on a regular basis in accordance with the Section of this Chapter on "Business Continuity Plan"; and
- systems and controls are in place to safeguard credit union assets against theft, burglary, vandalism and other physically hazardous conditions which may cause harm to officers, members or the assets of the credit union including putting in place at a minimum:

[1] See the Chapter on "Risk Management and Compliance".

- controls on access to the credit union premises including security procedures in relation to the opening and closing of the premises;
- procedures for the storage and transfer of assets and other valuables including cash;
- controls to minimise the threat of kidnapping and robbery; and
- health and safety procedures which are communicated to officers.

1.3.4 Reporting of operational risk

In order to ensure that operational risks are adequately monitored, the risk management officer should include in its reports to the board of directors (or risk committee where one exists) the following at a minimum:

- any operational risk exposures and losses;
- likely or actual deviations from risk tolerance levels;
- significant operational risk events and losses;
- relevant external events; and
- significant increase in operational risk exposure.

Where a significant operational risk event occurs, the risk management officer should bring this to the attention of the board of directors (or risk committee where one exists) immediately.

1.4 Risk register

The operational risks identified by the risk management system should be included in the credit union's risk register and managed in accordance with the credit union's overall risk management process.

1.5 EBA Guidelines on the Security of Internet Payments

Where a credit union provides the following internet payment services to members:

- [cards] the execution of card payments on the internet, including virtual card payments, as well as the registration of card payment data for use in 'wallet solutions';
- [credit transfers] the execution of credit transfers on the internet;
- [e-mandate] the issuance and amendment of direct debit electronic mandates; and
- [e-money] transfers of electronic money between two e-money accounts via the internet.

The credit union is expected to comply with the Guidelines issued by the EBA on the security of internet payments ("the Guidelines"). The Guidelines also provide examples of best practice which are encouraged but are not required to be followed.

Payments that are **excluded** from the scope of the Guidelines include payments where the instruction is given by post, telephone order, voice mail or using SMS-based technology. Other exempt payments are set out on page 10 of the Guidelines.

The Guidelines are effective from **1 August 2015**. Credit Unions should ensure that the requirements under these Guidelines are incorporated into the risk management processes set out in section 1.3 above.

2. Business Continuity Plan

2.1 Legislation

Section 76I – Business continuity plan*

(1) In this section—

'business continuity', in relation to the occurrence of one or more abnormal events which could cause a material interruption to the business of a credit union, means the continuation of its business during and after such an occurrence;

'business continuity plan', in relation to a credit union, means the contingency arrangements put in place to ensure that its essential functions can continue during and after the occurrence of one or more abnormal events which could cause a material interruption to the business of the credit union.

(2) A credit union shall put in place a business continuity plan—

(a) to ensure its business continuity if there occurs one or more abnormal events which could cause a material interruption to its business, and

(b) to enable it to continue to meet all requirements imposed on it under the *Credit Union Acts 1997 to 2012* and other financial services legislation if any such interruption occurs,

and such plan shall include, where appropriate, comprehensive testing at regular intervals of recovery procedures by officers of the credit union and testing of backup facilities.

Section 55 – Functions of board of directors*

(*This Chapter has not reproduced the entirety of section 55 – please consult the Credit Union Act, 1997 for the full provision)*

(1) Without prejudice to the generality of section 53(1), the functions of the board of directors of a credit union shall include the following:

…

(o) approving, reviewing, and updating, where necessary, but at least annually, all plans, policies and procedures of the credit union, including the following:

…

(xii) business continuity plan;

…

2.2 Guidance

The purpose of a business continuity plan is to ensure that when an interruption occurs a credit union can maintain essential activities and services including preserving essential data and functions and can:

- manage the initial interruption;
- recover lost data and functions and ensure the timely resumption of interrupted services and activities; and
- continue to meet all legal and regulatory requirements and guidance during the interruption.

2.3 The business continuity plan

The business continuity plan should cover the following at a minimum:

- objectives and scope of the plan;
- organisational arrangements setting out the roles and responsibilities of officers involved in business continuity;
- identification of resources required (people, systems, facilities and other assets and procedures) to continue critical operations taking account of the nature, scale, complexity and risk profile of the credit union;
- a business impact analysis (see the Section of this Chapter on "Business impact analysis" below);
- recovery strategies (see the Section of this Chapter on "Recovery strategies" below);
- testing of the business continuity plan (see the Section of this Chapter on "Testing of the business continuity plan" below);
- internal and external communication arrangements including escalation plans;
- annual training of officers involved in business continuity;

- business continuity plan for outsourced activities in accordance section 76J(7) of the 1997 Act;[2]
- insurance arrangements in place and insurance notification procedures to be followed in the event of loss from material interruptions;
- arrangements for the secure off-site storage of the business continuity plan;
- reporting arrangements, including the frequency, form and content of reporting on business continuity to the board of directors; and
- the process for the approval, review and update of the business continuity plan by the board of directors (see the Section of this Chapter on "Review and update of the business continuity plan" below).

The business continuity plan should be dynamic and flexible to allow for changes throughout the year. Credit unions should ensure that any significant deviations from the business continuity plan during a business continuity event or business continuity testing are communicated to the board of directors along with the reasons for these deviations and proposed action to address the deviations in accordance with the reporting arrangements set out in the business continuity plan.

The board of directors should ensure that the business continuity plan is communicated to all officers of the credit union.

2.4 Business impact analysis

A credit union should consider the likelihood, impact and resulting severity of an interruption to the continuity of its operations from abnormal events. This should include assessing the interruptions to which it is particularly susceptible, the likely timescale of those interruptions and the financial, operational and reputational impact of those interruptions. Interruptions may include the following at a minimum:

- the loss or failure of internal or external resources (such as people, systems and other assets);
- the loss or corruption of data; and
- any other events including vandalism, hacking or natural disasters.

The business impact analysis should cover the following at a minimum:

- identifying critical business activities;
- undertaking a risk assessment to assess the risk and impact of various interruption scenarios on the credit union's operations, regulatory compliance, finances, members' savings and reputation;

[2] See the Chapter on "Outsourcing".

- defining the maximum allowable downtime for critical business activities and the acceptable level of losses;
- establishing planned recovery levels and time frames for recovery and resumption of functions; and
- identifying key internal and external dependencies including third party service providers.

Maximum allowable downtime and planned recovery levels and timeframes identified in the business impact analysis should be reflected in outsourcing agreements where such functions are outsourced.

2.5 Recovery strategies

Following completion of the business impact analysis, the board of directors should develop recovery strategies which should cover the following at a minimum:

- emergency reaction and recovery procedures;
- communication arrangements including escalation plans;
- information systems continuity plans and recovery processes and data back-up and storage strategies; and
- processes to validate the integrity of information affected by the interruption.

2.6 Testing of the business continuity plan

A credit union should test the business continuity plan on a regular basis. The roles and responsibilities of officers involved in the test should be clearly defined. Tests should be monitored by an independent party such as the internal audit function or auditor and should, at a minimum:

- take place at least annually or when significant changes take place such as significant changes in business activities, responsibility, systems, facilities, personnel, outsourcing arrangements or the external environment;
- determine whether the credit union can recover to the extent envisaged in the continuity plan within the timeframe set out in that plan;
- test the restoration of data back-ups, simulations and alternative site reviews, where appropriate; and
- identify any gaps and failures in the business continuity plan and update the business continuity plan to address these gaps and failures.

The results of the test should be documented and reported to the board of directors.

2.7 Review and update of the business continuity plan

This review by the board of directors should cover the following at a minimum:

- assessing the scope and adequacy of the business continuity plan;
- evaluating the testing of the business continuity plan;
- ensuring that, following testing, appropriate follow-up and corrective actions have been taken; and
- ensuring the business continuity plan is updated as a result of the review.

3. Records Management

3.1 Legislation

Section 108 – Accounting records etc.

(1) Every credit union shall—

(a) cause proper accounting records, whether in the form of documents or otherwise, to be kept on a continuous and consistent basis, that is to say, the entries shall be made in a timely manner and be consistent from one year to the next, and

(b) establish and maintain systems of control of its business and records, in accordance with this section and section 109.

(2) The accounting records of a credit union shall be such as—

(a) correctly to record and explain the transactions of the credit union;

(b) to disclose, with reasonable accuracy and promptness, the financial position of the credit union at any time;

(c) to enable the officers properly to discharge the duties imposed on them by or under this Act;

(d) to enable the credit union properly to discharge the duties imposed on it by or under this Act; and

(e) to enable the accounts of the credit union to be readily and properly audited.

(3) Without prejudice to the generality of *subsections (1)* and *(2)*, accounting records kept pursuant to this section shall contain—

(a) entries from day to day of all sums of money received and expended by the credit union and the matters in respect of which the receipt and expenditure take place;

(b) a record of the assets and liabilities of the credit union and entries from day to day of every transaction entered into by the credit union which will or may give rise to liabilities or assets of the credit union; and

(c) in respect of the provision of services, whether under *section 48* or otherwise, a record of the services provided and all transactions relating to them.

(4) For the purposes of *subsection (1)* proper accounting records shall be deemed to be kept if they comply with *subsections (2)* and *(3)* and give a true and fair view of the state of affairs of the credit union and explain its transactions.

(5) The accounting records of a credit union—

(a) shall be kept at the registered office of the credit union or at such other place in the State as the board of directors think fit; and

(b) ‡ shall at all reasonable times be open to inspection by the members of the board of directors and the board oversight committee.

(6) Every record required to be kept under this section shall be preserved by the credit union for not less than six years from the latest date to which it relates.

(7) ‡ Where the accounting records of the credit union are kept at a place other than the registered office of the credit union, the chair shall have responsibility for ensuring that a written record of their location is kept.

(8) Where a credit union conducts its business in more than one place, the board of directors shall ensure that such accounting records are kept and such systems of control are established and maintained for each of those places as will enable the credit union to comply with this section and *section 109*.

(9) A credit union shall take adequate precautions to ensure the safe keeping of the accounting records of the credit union no matter what form they may take.

Section 109 – Systems of control and safe custody

(1) The systems of control which are to be established and maintained by a credit union pursuant to *section 108 (1)* are systems for the control of the conduct of its business as required by or under this Act and in accordance with the decisions of the board of directors and for the control of the accounting and other records of its business.

(2) Without prejudice to the generality of *section 108 (1)*, the systems of control must be such as to secure that the credit union's business is so conducted and its records so kept that—

(a) the information necessary to enable the officers, the credit union and the auditor to discharge their functions is sufficiently accurate, and is available with sufficient regularity and with sufficient promptness for those purposes, and

(b) ‡ the information obtained by or furnished to the Bank is sufficiently accurate for the purposes for which it is obtained or furnished and is available as and when required by the Bank.

(3) Every credit union shall establish and maintain a system to ensure the safe custody of all documents of title belonging to the credit union.

Section 76F – Records management*

(1) Without prejudice to sections 108 and 109, a credit union shall ensure—

(a) that it makes, maintains and retains in books and documents proper and secure records of all matters that are required to enable the credit union, including the board of directors, board committees, nomination committee and officers and its board oversight committee and auditor to discharge their respective functions and as required by law,

(b) that those records are made in a timely, accurate and consistent manner so that—

(i) they contain the information necessary to enable persons discharging functions to which paragraph *(a)* relates to discharge their respective functions and that those records are sufficiently accurate and available with sufficient regularity and sufficient promptness for the purpose of so discharging, and

(ii) any information furnished or caused to be furnished by or on behalf of the

credit union to the Bank is sufficiently accurate for the purposes for which it was so furnished and is available as and when required by the Bank, and

(c) that those records are produced when duly called upon—

(i) by or under this Act, or

(ii) for the purposes of any other statutory obligation to produce them.

Section 186 – Records and registers

(1) ‡ A credit union shall maintain, in addition to the records required to be kept by a credit union by virtue of section 108, such other records as may be prescribed by the Bank.

(2) Any register or record required to be kept by or under this Act may be kept either by making entries in bound books or by recording the matters in any other manner, provided that the recording is readily accessible and readily converted into written form in an official language of the State.

(3) Any duty imposed by this Act [or Part 3 of the Central Bank (Supervision and Enforcement) Act 2013] to allow inspection of, or to furnish a copy of, a record, or any part of it, is to be treated as a duty to allow inspection of, or to furnish, a reproduction of the recording or of the relevant part of it in a written form in an official language of the State.

(4) Where any register or record required to be kept by or under this Act is not kept by making entries in a bound book but by some other means, adequate precautions shall be taken by the person required to keep the register or record for guarding against falsification and for facilitating the discovery of any falsification.

Section 55 – Functions of board of directors*

(*This Chapter has not reproduced the entirety of section 55 – please consult the Credit Union Act, 1997 for the full provision.)*

(1) Without prejudice to the generality of section 53(1), the functions of the board of directors of a credit union shall include the following:

…

(o) approving, reviewing, and updating, where necessary, but at least annually, all plans, policies and procedures of the credit union, including the following:

…

(x) records management policies;

…

3.2 Guidance

3.2.1 Records management policy

The records management policy should cover the following at a minimum:

- the objectives of the credit union's records management policy;
- organisational arrangements setting out the roles and responsibilities of officers involved in records management;
- form and content of credit union records and the medium that records are to be recorded on;
- retention periods for records;
- procedures for:
  - the storage, transfer, duplication, back-up and disposal of records;
  - ensuring there is an audit trail for records and transactions to enable the credit union to evidence historical changes to records relating to member accounts, transactions of the credit union and accounting records;
  - the security, destruction and disposal of records;
  - handling requests for information;
  - protecting the integrity of records in situations of severe damage and/or interruption to the business of the credit union;
- schedule of records including the location of records held by the credit union;
- reporting arrangements, including the frequency, form and content of reporting to the board of directors; and
- the process for the approval, review and update of the records management policy by the board of directors.

Credit unions should ensure that any significant deviations from the records management policy, the reasons for these deviations and proposed action to address the deviations are communicated to the board of directors in accordance with the reporting arrangements set out in the records management policy.

4. Information Systems

4.1 Legislation

Section 76G – Information systems*

(1) In this section 'information systems', in relation to the business of a credit union, means all the technical and non-technical methods of establishing, implementing, documenting and maintaining data and information within the credit union in a coherent and informative way which is in, or capable of being reproduced in, a legible form.

(2) For the purpose of supporting the strategic plan and enabling the board of directors of a credit union and other persons involved in the management of the credit union to control, direct and manage its affairs, a credit union shall, taking account of the nature, scale and complexity and risk profile of its business but without prejudice to any other statutory obligation to the like effect as this section—

(a) develop, prepare, implement and maintain secure and reliable information systems, or

(b) where such systems already exist within the credit union, continue to implement and maintain such systems.

4.2 Guidance

Information systems of a credit union should, at a minimum, have the capability to:

- support the implementation of the strategic plan;
- provide accurate, reliable, consistent, timely and comprehensive information to enable the board of directors and the management team to monitor and analyse the financial position and performance of the credit union against the financial projections, targets and criteria contained in the strategic plan;
- record all transactions accurately and on a timely basis;
- support the credit union in monitoring compliance with all legal and regulatory requirements and guidance;
- provide an audit trail for all transactions to ensure compliance with the audit, record management and record retention requirements of the credit union including legislative requirements and guidance;

- protect the security of the information systems through appropriate access and process controls; and
- be capable of modification to facilitate changes such as changes to products and services, where appropriate, and the introduction of new regulatory requirements.

The board of directors should ensure that the information systems in a credit union are appropriate having regard to the nature, scale, complexity and risk profile of the credit union.

4.2.1 Security of information systems

The security of information systems should be protected by ensuring, at a minimum, that:

- passwords are strong and are changed on a regular basis;
- all mobile devices (e.g. laptops, tablets, USB keys etc.) and back-up devices are encrypted to prevent data loss/theft;
- officers are granted such access as is appropriate to their role and responsibilities;
- remote access, access by third parties and physical access is controlled, monitored and reviewed;
- audit trails of information system access are monitored and reviewed;
- the credit union receives timely notifications where the system has detected unauthorised use or tampering and violation attempts are recorded;
- resources, including people, processes and systems, are put in place to ensure the security of information systems taking account of the nature, scale, complexity and risk profile of the credit union;
- information systems penetration tests, to test the security controls in place to protect information systems against unauthorised access, are carried out where appropriate and vulnerabilities identified are rectified in a timely manner;
- systems are protected against information security incidents including data leakage, fire, vandalism and theft, equipment failure, unauthorised access or tampering, fraud, computer viruses and malicious software;
- training is provided to officers using the information systems; and
- information systems are secure in the event of a system interruption.

Credit unions should monitor the security of information systems and ensure any information system security incidents are reported to the board of directors.

4.2.2 Development of information systems

Any proposed change to information systems should be planned, documented, managed, authorised at an appropriate level and should not involve undue risk to the credit union and its operations. The board of directors of a credit union should not consider any new

information systems project unless the board of directors has fully satisfied itself that the credit union has the resources, financial and non-financial, and capacity to implement the project taking account of the nature, scale, complexity and risk profile of the credit union. Where information systems are updated or changed, or where new users are introduced, the credit union should ensure that comprehensive training is provided to users.

4.2.3 Maintenance of information systems

Credit unions should undertake a review to ensure information systems support the strategic plan on a regular basis, at least annually. Any enhancements required arising from the review should be made to information systems. Credit unions should ensure that the information systems, including hardware and software, are adequately supported, maintained and updated to ensure that they remain reliable on an ongoing basis.

4.2.4 Outsourcing

Credit unions should comply with the provisions of section 76J of the 1997 Act[3] when outsourcing any activities in relation to information systems. Credit unions should ensure at a minimum that:

- an appropriate level of support is available from the service provider;
- training, including manuals and materials, is provided to the credit union; and
- the information systems provided by the service provider meet current requirements and can be adapted to meet future requirements.

5. Management Information

5.1 Legislation

Section 76H – Management information*
(1) Without prejudice to any other statutory obligation to the like effect as this section, a credit union shall ensure that its information systems (within the meaning of section 76G) produce management information and other reports that are accurate, reliable, consistent, and timely so as to enable the board of directors and management team to— *(a)* direct, control and manage the credit union's business efficiently and effectively, *(b)* make informed strategic and operational decisions, and *(c)* provide accurate information to the Bank on a timely basis, as and when required.

[3] See the Chapter on "Outsourcing".

5.2 Regulations

CREDIT UNION ACT 1997 (REGULATORY REQUIREMENTS) REGULATIONS 2016 (S.I. No. 1 of 2016)

PART 8

SYSTEMS, CONTROLS AND REPORTING ARRANGEMENTS

Plans, Policies and Procedures

46. (1) A credit union shall establish and maintain, in writing, all policies specified in section 55(1)(o) of the Act.

(2) A credit union shall ensure that the matters specified below shall be communicated to all officers in the credit union following any updates made, including the review, approval and update by the board of directors required at least annually of:

(a) the risk management policy;

(b) the business continuity plan;

(c) the conflicts of interest policy; and

(d) the standards of conduct and ethical behaviour of officers.

(3) A credit union shall document, approve and update, at least annually, the matters specified in Schedule 1 to these Regulations.

(4) A credit union shall, at a minimum, establish and maintain information systems and management information policies which include:

(a) a management information policy;

(b) an information security policy;

(c) an information systems change management policy; and

(d) an information systems asset management policy.

SCHEDULE 1

1. The systems of control of its business and records required under section 108(1)(b) of the Act,
2. A succession plan for the board of directors and the management team which shall

detail the key skills and competencies required for members of the board of directors and management team,

3. The annual review of overall performance carried out by the board of directors as required under section 55(4) of the Act,
4. The annual compliance statement, together with supporting documentation used in the preparation of the compliance statement.

5.3 Guidance

Management information required to enable the board of directors and the management team to direct, control and manage the credit union's business effectively and efficiently and to make informed strategic and operational decisions should be produced on a regular basis, but at least monthly. Reports may need to be produced more frequently having regard to the nature, scale, complexity and risk profile of the credit union.

Management information should cover the following at a minimum:

- reports on the financial position of the credit union submitted by the manager under section 63A(4)(c) of the 1997 Act;[4]
- past performance, trends, and projections of the financial position of the credit union;
- strategies proposed by the manager under section 63A(4)(a) of the 1997 Act;[5]
- updates from the manager on the performance of the credit union against financial projections, targets and criteria set out in the strategic plan;
- membership and accounts of the credit union;

- reports of the activities of each board committee under section 56A of the 1997 Act;[6]
- reports from the board oversight committee required under section 76O(2) of the 1997 Act;[7]
- reports of the credit committee, credit control committee and membership committee required under the Third Schedule of the 1997 Act;
- reports from the risk management officer and from the compliance officer under sections 76C and 76D of the 1997 Act;[8]

[4] See the Chapter on "Governance".
[5] See the Chapter on "Strategic Plan".
[6] See the Chapter on "Governance".
[7] See the Chapter on "Governance".
[8] See the Chapter on "Risk Management and Compliance".

- reports received from the internal audit function under section 76K(5) of the 1997 Act;[9]
- reports on the results of tests carried out on the business continuity plan required under section 76I(2) of the 1997 Act;
- reports on the review of the performance of outsourced activities and agreements;[10] and
- any other reports required under financial services legislation.

The management information produced to enable the board of directors and management team to provide accurate information to the Central Bank on a timely basis, as and when required, should cover the following at a minimum:

- prudential returns;
- draft financial statements and final financial statements;
- annual return;
- annual audited accounts;
- AGM notifications; and
- outsourcing notifications (as required under section 76J of the 1997 Act).[11]

5.3.1 Review by the board of directors

The board of directors should assess and review the information systems that produce management information on a regular basis, at least annually, to ensure that the information produced is accurate, reliable, consistent, and timely and that the management information meets all legal and regulatory requirements and guidance.

[9] See the Chapter on "Internal Audit".
[10] See the Chapter on "Outsourcing".
[11] See the Chapter on "Outsourcing".

6. Information Systems and Management Information Policies

6.1 Legislation

Section 55 – Functions of board of directors*

(*This Chapter has not reproduced the entirety of section 55 – please consult the Credit Union Act, 1997 for the full provision.)*

(1) Without prejudice to the generality of section 53(1), the functions of the board of directors of a credit union shall include the following:

…

(o) approving, reviewing, and updating, where necessary, but at least annually, all plans, policies and procedures of the credit union, including the following:

…

(xi) information systems and management information policies;

…

6.2 Guidance

The information systems and management information policies required in a credit union should include the following at a minimum:

- management information policy;
- information security policy;
- information systems change management policy; and
- information systems asset management policy.

Each of these policies should cover the following at a minimum:

- objectives of the policy;
- organisational arrangements setting out the roles and responsibilities of officers involved; and
- the process for the approval, review and update of the policy by the board of directors.

The management information policy should also cover the following at a minimum:

- the management information reports to be produced including details on the frequency, form and content, distribution and management of management information reports;
- procedures in place:

  - to ensure the reliability, consistency, timeliness, accessibility and comprehensiveness of management information;
  - for the independent assurance that information systems produce accurate management information;
  - for the secure storage, back-up, transfer and disposal of management information in line with all legal and regulatory requirements and guidance, including data protection requirements and guidance;
  - to ensure compliance with legislative and regulatory requirements including data protection legislation; and
- a system for logging and rectifying errors in management information.

The information security policy should also cover the following at a minimum:

- resources required in respect of information security taking account of the nature, scale, complexity and risk profile of the credit union;
- how access to information systems (including remote access, third party access and physical access) will be controlled, monitored and reviewed such as the recording and maintenance of audit trails of access;
- security controls to prevent unauthorised access including password management, firewalls, virus protection and encryption of mobile and back-up devices;
- procedures in place for monitoring threats from both technical sources[12] and non-technical sources[13] and updating access and security controls as appropriate;
- procedures in place for the ongoing assessment and testing of access and security controls including information systems penetration tests, where appropriate, and the rectification of any vulnerabilities identified;
- procedures for managing information security incidents such as data leakage, fire, vandalism and theft, equipment failure, unauthorised access or tampering, fraud, computer viruses and malicious software;
- training to officers to ensure the accurate operation of information systems in a safe and secure manner; and
- reporting arrangements, including the frequency, form and content of reporting to the board of directors on information security.

The information systems change management policy should also cover the following at a minimum:

- processes to:

[12] Technical sources include new systems, new service providers, and increased access.
[13] Non-technical sources include organisational changes, business process changes, new business locations or new products and services.

  - assess information systems changes required, including changes required to support the credit union's strategic plan and to ensure that the credit union complies with all legal and regulatory requirements and guidance;
  - determine the business case for and impact of changes to information systems;
  - approve changes to be made to information systems;
  - select, where appropriate, information systems and service providers;
  - manage the implementation of information system changes including planning, designing, developing, testing implementing and supporting changes to information systems;
  - ensure any change is successfully tested prior to implementation, including parallel running[14] where appropriate;and
  - ensure the accuracy of information, including management information, is verified following implementation of any change;
- business continuity procedures in place in the event that changes to information systems cause interruption to the business of the credit union, including roll-back plans,[15] where appropriate;
- communication and training arrangements in relation to the introduction of proposed changes; and
- reporting arrangements, including the frequency, form and content of reporting on changes proposed and made to information systems to the board of directors.

The information systems assets management policy should also cover the following at a minimum:

- procedures for developing an information system asset register listing all information systems assets, including software licences, and identifying the assets that are critical to the business of the credit union;
- procedures in place to ensure compliance with the terms of the information systems contracts and licence agreements;
- succession and replacement plans for information system assets;
- processes to confirm the existence of all information system assets on a regular basis; and
- reporting arrangements, including the frequency, form and content of reporting on information systems assets to the board of directors.

Credit unions should ensure that any significant deviations from the information systems and management information policies, the reasons for these deviations and proposed action to address the deviations are communicated to the board of directors in

[14] A parallel run is where the existing information systems and the changed/updated information systems are run concurrently for a specified period of time to ensure expected results are consistent across the systems.
[15] A roll back plan allows a credit union to revert the information system back to the pre-change state.

accordance with the reporting arrangements set out in the information systems and management information policies.