ISLE OF MAN
FINANCIAL SERVICES AUTHORITY

Lught-Reill Shirveishyn Argidoil Ellan Vannin

GUIDANCE NOTE FOR DEPOSIT TAKERS

(Class 1(1) and Class 1(2))

Corporate Governance

March 2017

STATUS OF GUIDANCE

The Isle of Man Financial Services Authority ("the Authority") issues guidance for various purposes including to illustrate best practice, to assist licenceholders to comply with legislation and to provide examples or illustrations. Guidance is, by its nature, not law, however it is persuasive. Where a person follows guidance this would tend to indicate compliance with the legislative provisions, and vice versa.

Version 1.1

Contents

1. Introduction 3
2. Overview 3
3. Board practices 5
4. Senior management 14
5. Risk management and internal controls 15
6. Performance management and remuneration 18
7. Corporate structure, disclosure and transparency 19

Appendix 1 – Glossary 21
Appendix 2 - Useful Website Links – further reading 22

1. Introduction

1.1 This guidance applies to all deposit takers (hereinafter referred to as bank or banks as applicable) that are licensed by the Isle of Man Financial Services Authority ("the Authority") under the Financial Services Act 2008 to conduct Class 1(1) and Class 1(2) regulated activity.

1.2 This guidance is designed to apply as widely as possible to assist banks in enhancing their corporate governance frameworks. It is intended to reinforce the key elements of widely accepted and long established corporate governance principles that should guide the actions of directors and managers in a variety of banks, recognising that much depends on the size and complexity of the operations. *The guidance primarily links to Part 8 of the Financial Services Rule Book ("the Rule Book").*

1.3 Corporate governance refers to the processes, structures and information used for directing and overseeing the management of a company. Ultimately, corporate governance is about the behaviour of boards and their senior management. Good corporate governance is fundamental to sound and prudent management of banks.

1.4 Effective corporate governance and the effective exercise of the responsibilities of the board and senior management are key elements of the Basel Core Principles for Effective Banking Supervision, which are supported by the Authority. The Basel Committee has issued several papers relating to corporate governance (and risk management) which are accessible on its website www.bis.org.

1.5 The Authority has previously issued a guidance note on the responsibilities and duties of directors under the laws of the Isle of Man, which is addressed to all Isle of Man companies. That guidance note continues to apply and is relevant to banks incorporated in the Island.

1.6 Standards of corporate governance in a bank may be relevant to the Authority's assessment of the competence of the directors and other responsible officers.

2. Overview

2.1 From a banking industry perspective, corporate governance involves the manner in which the business and affairs of a bank are governed by its board of directors and senior management, including how they:

- set the bank's strategy and objectives
- determine the bank's risk tolerance / appetite
- operate the bank's business on a day to day basis

- meet the obligation of accountability to their shareholders and take account of the interest of other stakeholders[1]
- align corporate activities and behaviour with the expectation that the bank will operate in a safe and sound manner, and be in compliance with applicable laws and regulations
- protect the interest of depositors

2.2 Sound corporate governance is an essential element in the safe and sound functioning of a bank and may affect the risk profile of a bank if not implemented effectively.

2.3 Sound corporate governance also contributes to the protection of depositors of the bank.

2.4 Sound corporate governance practices are essentially important in situations where a bank is experiencing problems or where significant corrective action is necessary.

2.5 Sound corporate governance can be achieved regardless of the form of oversight used by a bank as long as several essential functions are in place. There are four important forms of oversight that should be included in the organisational structure of any bank to ensure appropriate checks and balances:

- oversight by the board of directors
- oversight by individuals not involved in the day to day running of the various business areas
- direct line supervision of different business areas
- independent risk management, compliance and audit functions

In addition it is important that key personnel are fit and proper and suitably experienced for their jobs.

2.6 *Local subsidiaries of international groups*

2.6.1 It is acknowledged that some banks operate to group policies and procedures. This guidance is not intended to create additional requirements but rather to set out some of the expectations in the Isle of Man.

2.6.2 Banks which are local subsidiaries of international financial services groups should have a clear understanding of group policies and the extent of their autonomy.

2.6.3 The specific guidance in sections 3 to 7 covers the relationship between a subsidiary and its group / parent in more detail where applicable.

[1] Supervisors, governments and depositors are among the stakeholders due to the unique role of banks in economies and financial systems, and the associated implicit or explicit deposit guarantees.

2.7 *Branches*

2.7.1 The obligation to operate to group / head office policies and procedures is particularly strong for branches. This guidance is not intended to create any additional requirements but rather to set out some of the expectations in the Isle of Man.

2.7.2 If the Isle of Man operation is a branch, then there should be clear direction set by the head office (which may be part of a division of the bank) that provides senior management with the authority to operate and a framework in which this works.

2.7.3 Having established the extent of their local management responsibilities, a bank should:

- address the standards and guidance referred to in sections 3 to 7; using its arrangements with the group to determine which of the functions are carried out by the local senior management and which are referred to the head office
- address the standards and guidance in sections 3 to 7 in ensuring that there is proper communication between the local senior management and head office
- branches in which the local senior managers delegate operational responsibility to other managers should address the relevant standards and guidance on proper control by directors where they delegate (substituting local senior management for the directors)

Sound corporate governance principles

3. Board practices

3.1 ***The board has overall responsibility for the bank, including approving and overseeing the implementation of the bank's strategic objectives, risk strategy, corporate governance and values, and providing oversight of senior management***

3.1.1 *Board responsibilities*

The board has ultimate responsibility for the bank's business, risk strategy and financial soundness, and should therefore, taking into the account the interests of shareholders, depositors and other relevant stakeholders:

- approve the business strategy of the bank
- approve and oversee the implementation of risk strategy and tolerance / appetite
- approve and oversee the implementation of risk policy, risk management and internal control systems

- approve and oversee the implementation of corporate governance principles and values

All directors should understand the regulatory environment, their oversight role, the bank's risk profile and the potential of conflicts of interest occurring.

3.1.2 *Oversight of senior management and control functions*

The board should provide oversight of senior management and should:

- monitor senior management's actions to ensure they are consistent with the strategy and policies approved by the board
- meet regularly with senior management
- question and review explanations and information provided by senior management
- set lines of responsibility and accountability throughout the bank which define clearly the responsibilities and authorities of the board, control functions and senior management
- regularly review policies, processes and controls with senior management and control functions to determine areas needing improvement, and to address significant risks and issues

The board should ensure that the control functions are properly staffed and resourced and are carrying out their responsibilities independently and effectively.

3.1.3 *Corporate values*

The board should encourage high standards of professional conduct. This can be achieved by setting appropriate standards and having policies to address any illegal, unethical or questionable behaviour by members of the board or staff. If a matter comes to the attention of a director or senior manager that leads them to conclude that another member of staff has acted in an inappropriate manner that could bring the bank or Island into disrepute this should be reported.

A whistle blowing regime / policy must be established with communication allowed to be made to the board (directly or indirectly – e.g. through an independent audit or compliance process) independent of the internal management reporting structure. Appropriate action should be taken to protect the whistle-blower from any negative repercussions arising from reporting in good faith their concerns. The confidentiality of any reports should be respected. The policy must also set out an internal reporting structure to enable the bank's responsible officers, key staff and all employees to raise concerns internally but outside of the normal management reporting structure; and include provisions requiring persons to whom it applies to raise their concerns directly with the Authority if they feel that they have not been adequately addressed internally.

A bank should ensure, by way of a policy, statement or procedures as applicable, that the withdrawal of money by directors from their personal accounts held with

the bank is treated no more favourably than withdrawals that would be made by any other customer. For example, requests for withdrawal by directors should not be given priority over the request of other customers, and any request to break the contractual terms of the deposit should be considered in line with the bank's general policy relating to term accounts for all customers, and in any event requests for withdrawals outside the terms of the deposit should be signed off by another director.

3.2 ***Board members should be and remain qualified, including through training, for their positions (including as a member of any committee), understand their role and be able to exercise sound judgement***

3.2.1 *Training and qualifications*

The board should possess, both as individual members and collectively, appropriate experience, competencies and personal qualities including professionalism and personal integrity. Examples of where the board should seek to have, or have access to, appropriate experience include finance, accounting, strategic planning, communications, governance, risk management, regulation, auditing and compliance.

It is good practice for all directors to receive or to have received training on their legal duties as directors and regulatory responsibilities prior to or shortly after being appointed to the board and be reminded of these on a periodic basis. This includes their responsibilities under the appropriate Anti Money Laundering legislation.

It is recommended that there is an induction programme for all non-executive directors and that they are able to challenge and test proposals on strategy, risk matters and can draw on any information they feel is relevant to understand a business.

A non-executive director's training and education requirements should be reviewed annually in line with the changing needs of the business.

3.2.2 *Composition*

Ideally a board should be comprised of an adequate number of directors with a balance of executive and non-executive directors (including group representatives where relevant and independent non-executive directors) so that no individual or small group can dominate the board's decision making.

Board members should be able to commit the necessary time and effort to fulfil their responsibilities.

3.2.3 *Non-executive directors*

Upon appointment, non-executive directors (including Group and independent directors) should receive a formal letter of engagement (or similar) from the bank, detailing the terms of their contract, and expectations of the non-executive director role including remuneration etc.

3.2.4 *Executive directors*

It is important that executive directors are aware of any additional director responsibilities which may be required of them in addition to their normal job role, particularly requirements of attendance at board meetings. A contract (or similar) should be agreed, which sets out the terms and conditions of the executive director acting as a board member (separate from their job role/specification).

3.2.5 *Independent non-executive directors*

At least one director of an Isle of Man incorporated bank must be of independent non-executive status (see Rule 8.35 (2) of the Rulebook).

Although the detailed knowledge and experience of a bank's affairs may be less for an independent non-executive director than an executive director or group non-executive director, the board's independence and objectivity can be enhanced by including non-executive members on the board who are capable of exercising sound judgement. This can be particularly important in areas where there is a risk that the board could be dominated by senior executive directors or where there is potential for conflict of interest in key areas (e.g. financial and non-financial reporting, related party transactions, nomination of board members and key executives and compensation arrangements).

In order to ensure there is an adequate level of challenge to the executive team, the Authority considers that there should be an appropriate level of knowledge and experience of the financial services industry, including banking, within the group of appointed independent non-executive directors.

For a non-executive director to be considered independent they should:

- be independent in character and judgement and not have a material business relationship with the bank (nor had one within the previous 3 years)
- not have been an employee of the bank or group within the last 5 years
- not hold cross directorships or have significant links with other directors through involvement in other companies or bodies
- not receive any additional remuneration or benefits apart from a director's fee
- not have close family ties with any of the bank's advisors, directors or senior employees
- not represent a significant shareholder
- not normally serve for more than 9 years from the date of their election

An independent non-executive director should:

- have a sufficient understanding of the bank's policies, key risks, control environment and key regulatory requirements in order to evaluate management information and generally oversee the operation of the bank
- receive ongoing training as appropriate in relation to the bank's policies and AML/CFT training as required by the relevant legislation in force
- scrutinise the performance of management in meeting agreed goals and objectives and monitor the reporting of performance

3.2.6 *'De Facto' Directors*

External parties can sometimes regularly attend, and take an active role in board meetings. This could lead to the risk that they are regarded as a 'de facto' director (as outlined in the guidance note on the responsibilities and duties of directors under the laws of the Isle of Man), and assume personal liabilities as a result of this.

Banks should be cautious in such situations, to ensure the 'de facto' director risk does not materialise.

3.2.7 *Continued Professional Development ("CPD")*

It is good practice for all directors and key persons to maintain appropriate levels of CPD, currently a minimum of 25 hours relevant CPD per annum. This assists them in keeping up to date with current developments and best practice. Under Rule 8.5 of the Rule Book the bank is also required to ensure that all directors comply with certain CPD requirements, and the bank must also maintain records to evidence the CPD compliance for these individuals.

3.3 ***There should be appropriate governance practices for the board's own work and the board should be supplied with quality timely information to allow for effective monitoring and control of the bank***

3.3.1 *Organisation and structure*

The board should structure itself in an appropriate way to enable matters to be:

- addressed efficiently
- reviewed in depth where required
- critically challenged and discussed

This structure should take into account the board's size, frequency of meetings (see 3.3.6), and use of committees (see 3.3.3, 3.3.4 and 3.3.5).

3.3.2 *The chair of the board*

The chair of the board should be responsible for the board's effective overall functioning. The chair should ensure that board discussions are taken on a sound and well informed basis and promote critical discussion and views of all directors.

It is increasingly common for the chair to be a non-executive and this practice is encouraged by the Authority.

3.3.3 *Board committees - general*

A board may find it beneficial to establish specialised committees to advise it. The number and nature of committees will depend on factors such as the size of the bank and the board, the nature of the business of the bank and its risk profile.

Where committees of the board are established their mandate, composition (including any members who are considered to be independent) and working procedures should be well defined.

3.3.4 *Audit committee*

If it is considered appropriate the board should establish a specific audit committee. The members of an audit committee should ideally comprise non-executive directors who are independent of management and have a firm understanding of the role of the audit committee.

The primary responsibilities of the audit committee should be oversight of the bank's internal and external auditors, reviewing and approving audit scope and frequency, receiving audit reports and ensuring management is taking appropriate actions in a timely manner to address identified weaknesses.

3.3.5 *Other committees*

Other specialised committees that are common (depending on the nature and size of the bank) are:

- risk management committee – to provide oversight of senior management's activities in managing credit, capital, market, liquidity, operational, compliance, reputation and other risks of the bank (sometimes a separate compliance committee is established)
- compensation / remuneration committee – to provide oversight of remuneration of senior management and other key personnel to ensure remuneration is consistent with the bank's culture, objectives, strategy and control environment, and that the remuneration policy as required by Rule 8.6(A) is appropriate and complied with
- nominations / corporate governance / human resources committee – to provide an assessment of board effectiveness and direct the process of renewing and replacing board members

Non-executive directors, as well as other directors with appropriate skills and knowledge, may play a key role on such board committees.

3.3.6 *Frequency of meetings and recording of information*

It is recommended that the board meets not less than quarterly, and more frequently where this is appropriate to the bank.

Board meetings should have a structured agenda which, together with the supporting papers, should be circulated some days in advance of the meeting. The board should consider specifying what it requires to be included in standard board agendas as well as the frequency that such matters should appear on such agendas. The company secretary or an executive of the bank should be designated as being responsible for ensuring effective and timely information flows to the board (and its committees) and executive management. Minutes of each meeting should be recorded, and action points should be clearly defined, carried forward and tracked to resolution.

The agenda should enable the board to adopt and review in an orderly fashion the policies necessary to meet the various statutory and regulatory requirements, updating these policies as appropriate.

The board should record its consideration of significant issues and decisions made relating to ongoing operations and material transactions.

Where roles which are important to meeting regulatory requirements, such as compliance officer, MLRO or company secretary are held by non-directors, there should be clear arrangements for the post-holders to report to the board on their respective responsibilities. Arrangements should be made for the post-holders to have direct access to the board including for presenting their reports to the board.

Banks should encourage regular attendance of all directors at board meetings and monitor levels of attendance. Directors should aim to attend board meetings in person wherever possible.

The board should document in its minutes any matters that it is delegating.

When delegating responsibilities, the directors need to remember that they remain accountable and should put in place a mechanism to receive information on the delegated activities as appropriate.

The directors and senior management should be aware of the items / matters which need to be referred to the board and documented. Where directors have concerns which cannot be resolved they should ensure that these concerns are recorded in the board minutes.

3.3.7 *Conflicts of interest policy*

Rule 8.9 of the Rule Book requires banks to maintain a conflicts of interest policy. In addition to this policy the board should agree standards of expected behaviour. All directors should maintain high standards of business conduct, integrity, and ethical behaviour and operate with due care and diligence.

The policy should include, where relevant:

- a review or approval process for members to follow before they engage in certain activities (e.g. serving on another board) to ensure such an activity will not create a conflict
- a member's duty to disclose any matter than may result, or has resulted, in a conflict of interest
- a member's responsibility to abstain from voting on any matter where the member may have a conflict of interest
- a process by which members disclose outside interests, including those of close family members (e.g. other directorships, shareholdings, membership of bodies etc) on a regular basis, and that these interests should be reviewed for any potential conflicts of interest
- adequate procedures for transactions with related parties on an arms-length basis
- the way in which the board will deal with any non-compliance with the policy

Examples of where conflicts may arise can be useful to include in a policy.

The Authority would also expect there to be a reminder issued to staff of their responsibilities under this policy on a regular basis.

3.3.8 *Recording conflicts of interest*

Rule 8.10 of the Rule Book requires banks to maintain a conflicts of interest register. Banks should ensure that all conflicts notified to, and considered by them, are recorded within this register in order that they can demonstrate that the conflicts are being managed appropriately.

The Authority also expects banks to obtain details of any external directorships and other interests held by their directors (including non-executive directors) and employees. Any returns provided in this regard should be reviewed to ensure that any matter which may give rise to a conflict of interest is identified, disclosed and managed accordingly. Any potential conflicts of interest for directors should be disclosed at the commencement of board meetings, based upon the agenda and matters to be discussed, in order to determine whether the conflict means certain directors should exclude themselves from parts of the meetings and/or abstain from voting on specified matters.

The board should ensure that the policy established under rule 8.9, and the register maintained under rule 8.10, of the Rule Book, are reviewed annually or

more frequently where appropriate. In accordance with Rule 8. 23 (d) of the Rule Book, the Compliance Officer of a bank is responsible for ensuring the conflicts of interest register is maintained.

3.4 *The board should set and enforce clear lines of responsibility and accountability in relation to its group structure*

3.4.1 *Interaction and relationship between the subsidiary bank and parent / group*

In the Island, most banks are subsidiaries of banks / banking groups headquartered in another jurisdiction. Normally, the board of a subsidiary bank in the Island should adhere to the same corporate governance principles as those expected of its parent / group company (subject to proportionality). The Authority recognises that the corporate governance structures and activities of the bank may be integrated with, and influenced by, those of the parent and group.

It is expected that a subsidiary bank in the Island will be subject to oversight by the parent / group.

The subsidiary (local) board should retain and set its own corporate governance responsibilities, and should evaluate any group-level decisions or practices to ensure that they do not put the subsidiary bank in breach of applicable legal or regulatory provisions. The local board should also ensure that such decisions are not detrimental to:

- the sound and prudent management of the subsidiary bank
- the financial health of the subsidiary bank
- the legal interests of the subsidiary bank's stakeholders

3.4.2 *Business line and matrix management*

For a subsidiary bank in the Island the corporate governance structures and activities of the bank may be integrated with, and influenced by, those of the parent or other subsidiaries.

Many groups now operate on a matrix and business line management structure that may not coincide with the bank's legal entity structure (e.g. employees have dual reporting lines to both business line and legal entity management). Such structures may be effective and serve useful business and control purposes for the group but may pose challenges to the effective corporate governance of the bank (for example there may be gaps in responsibility and accountability for the subsidiary bank within the group structure). The board and senior management should ensure that the decisions of matrix and business line management structures are consistent with proper fulfilment of the bank's own corporate governance responsibilities.

3.4.3 *Outsourcing of key risk functions*

Where a bank outsources key risk functions the accountability of the directors and senior management cannot be delegated to the entities providing the outsourced services[2]. Intra-group outsourcing of functions such as internal audit, compliance and risk management oversight / operational assurance does not remove the bank's obligations with respect to maintaining adequate oversight functions (which can be outsourced) and does not eliminate the board's responsibility for understanding and managing the risks in the bank.

4 Senior management

4.1 *Senior management should ensure that the bank's activities are consistent with the business strategy, risk appetite and policies approved by the board*

4.1.1 *Constituents of senior management*

Senior management is considered to consist of a core group of individuals who are responsible and should be accountable for overseeing the day to day management of the bank. Senior management includes, for example, the chief financial officer (or equivalent) and divisional / functional / business heads. These individuals should have the necessary skills to manage the business under their supervision and have appropriate control over the key individuals in their areas.

4.1.2 *Roles and responsibilities*

Senior management should set the "tone at the top" along with the board through their own personal conduct.

Senior management should oversee line managers (and delegate duties to them that promotes accountability) in specific business areas and activities consistent with the strategy, risk tolerance, policies and procedures set by the board.

Senior management should implement appropriate systems for managing the risks to which the bank is exposed, including an effective system of (independent) risk management and internal controls (this is addressed in more detail in section 5).

4.1.3 *Continued Professional Development ("CPD")*

It is good practice for all senior managers to maintain appropriate levels of CPD. This assists them in keeping up to date with current developments and best practice. Under Rule 8.5 of the Rule Book the bank is also required to ensure that all key persons comply with certain CPD requirements.

[2] Refer to the Authority's guidance note on outsourcing / delegation of functions.

It is the responsibility of senior management to ensure that individuals within the bank have the appropriate level of training and (if appropriate) a development framework.

5 Risk management and internal controls

5.1 *Banks should have an independent risk management function with sufficient authority, independence, resources and access to the board*

5.1.1 *Overview*

Risk management encompasses the process of identifying key risks to the bank, measuring and monitoring exposures to those risks (which may link to capital planning and ICAAP), taking steps to control / mitigate risks and appropriate reporting to senior management and the board.

Internal controls are designed to ensure that each key risk has a process or other measure to help contain or control the risk and that such process or measure is applied properly and works as intended. Internal controls help avoid actions being taken beyond the authority of an individual, mitigate fraud, help prevent money laundering and place checks on discretions. Even in very small banks key management decisions should be taken by more than one person.

5.1.2 *Chief risk officer (CRO) (or equivalent)*

Depending on the bank's risk profile and size it should have an independent senior executive with responsibility for the risk management function and the bank's risk management framework. In larger banks the role should ideally be distinct from other executive functions and business line responsibilities. The CRO should be of sufficient stature and seniority within the bank.

The CRO should report and have direct access to the board and any relevant committee (e.g. risk committee) and such interaction should be regular. The CRO may have other reporting lines too (such as to other senior management or executive directors). Non-executive directors should have the right to meet with the CRO in the absence of others.

It is however recognised that the CRO may not be based in the Island (i.e. may be part of a wider group function with responsibility for the Isle of Man subsidiary bank).

5.1.3 *The risk management function*

The risk management function should be responsible for identifying, measuring, monitoring, controlling or mitigating, and reporting on risk exposures.

The risk management function should be sufficiently independent of the business units whose activities and exposures it reviews. It is however important that risk

managers are not isolated from business units and it is recognised that it is not uncommon for risk managers to work closely with individual business units and to have dual reporting lines.

The risk management function should ultimately be responsible to the board and issues raised by it should receive the appropriate attention from the board, senior management and business units.

The function should be adequately resourced both from a systems and staffing perspective (including managers who possess sufficient experience, knowledge and qualifications where appropriate)[3].

5.2 ***Risks should be identified and monitored appropriately in accordance with the bank's risk profile and there should be reporting to the board and senior management***

5.2.1 *Risk methodologies and activities - general*

Risk analysis should include both quantitative and qualitative elements and include stress testing and a range of scenarios where applicable. Specific guidance on stress testing for capital is addressed in the Authority's guidance note on ICAAP, and for liquidity within the Authority's guidance note on liquidity risk management.

The risk management function should promote the importance of senior management and business line managers in identifying and assessing risks critically.

5.2.2 *Risk methodologies and activities – specific application to subsidiary*

In the Island, most incorporated banks are subsidiaries of larger financial services groups. For a subsidiary bank the board and senior management of the subsidiary remain responsible for effective risk management processes at the subsidiary. The local management and board should therefore have appropriate input into any local or regional adoption of risk methodologies and to assessments of local risks.

Irrespective of the use of any group / parent models and reporting frameworks the daily operational management of risk cannot be delegated away from the subsidiary and the subsidiary should have adequate tools in place and understand its reporting obligations to its parent / group.

5.2.3 *New products, business lines, acquisitions etc*

A bank should have an approval process for new products to include an assessment of the target client type, risks, significant changes to existing products,

[3] Some banks encourage or require staff to serve in both business line and risk management roles (e.g. on a rotational basis for development). Such an approach is considered to have several benefits including the promotion of the stature of risk management within the bank.

the introduction of new business lines and entry into new markets. The local and/or group (as appropriate) risk management and compliance function(s) should provide input on risks as part of the process.

The process should take into account the extent to which the bank's risk management, legal and regulatory compliance, systems, business line and internal control functions have adequate tools and expertise to manage related risks arising. New products and business lines should be delayed until such time that systems etc can accommodate the activity.

The risk management function should be actively involved in assessing risks that could arise from mergers and acquisitions and should report findings to the board. In particular, risks can arise from conducting insufficient due diligence that fails to identify risks that arise post-merger.

5.2.4 *Reporting to the board (committees) and senior management*

Information should be communicated in a timely, complete, understandable and accurate manner to enable the board to make informed decisions and, where necessary, take prompt and critical decisions. There should be a balance between communicating information that is accurate and unfiltered (i.e. does not hide potential bad news) and not communicating so much that the sheer volume becomes counterproductive.

Risk reporting to the board should ensure that bank wide and individual business / portfolio risks are conveyed in a meaningful manner. Results of stress tests and scenario analysis, where undertaken, should be communicated to aid discussion on the bank's current and potential exposures. Market conditions and trends should also be taken into account where applicable.

Risk reporting at subsidiary level may also be used as part of a wider group risk reporting methodology and reported accordingly to the parent / group.

5.3 *The board and senior management should effectively utilise the work conducted by the internal audit function, external auditors and other internal control functions*

5.3.1 *Internal / External Audit function*

All banks are required to have an internal audit function. This can take the form of one or more of the following:

- an in-house internal audit function
- where part of a larger group the group's internal audit function
- outsourced to a third party, for example a firm of accountants

Irrespective of the form of the internal audit function the board should review the arrangements at least annually to ensure that they are appropriate for the size and nature of the bank's operations.

The Authority believes the relationship between internal audit, external audit and itself are very important. Each can assist the other in discharging their respective duties and responsibilities. It is the normal practice for the internal audit and external audit to liaise at least on an annual basis.

Where appropriate the Authority will rely on work undertaken by the internal audit function and might request internal audit to undertake particular tasks and report to it.

For internal audit to be effective it should have direct access to the board or an audit committee. It may be beneficial for independent non-executive directors to meet in the absence of bank management at least annually with the external auditor and the heads of internal audit and compliance.

There should be clear processes for tracking any issues raised by internal audit, particularly in terms of local responsibilities and reporting to the board. Good quality reporting helps to provide assurance to the board that all issues raised are being dealt with appropriately.

Also refer to section 3.3.4 re audit committee and the requirements laid down in Rule 8.34.

5.3.2 *Sound internal control functions*

The bank should maintain sound internal control functions including an effective compliance function that monitors compliance with corporate governance rules, regulations, codes and policies to which the bank is subject and reports issues to an appropriate level of management within the bank or, if appropriate, to the board.

6 Performance management and remuneration

6.1 *Remuneration policies and practices should be consistent with the bank's corporate culture, long term objectives, strategy and control environment*

6.1.1 The board should approve policies that are consistent with effective risk management and avoid creating incentives that encourage excessive risk taking or are related to short term gains.

Incentive / bonus schemes can be an important indicator of what the bank values and a key influence on its culture. Rule 8.7 sets out the key matters that a remuneration policy has to contain, and banks should ensure that their incentive / bonus schemes are properly controlled and are not structured in a way that could create risks of staff selling products to customers that they do not need or want.

Incentive / bonus schemes should be designed carefully with good customer outcomes in mind, and the risks they pose should be identified and managed properly.

6.1.2 To help achieve this culture, the Authority believes it is important that the role profile and performance objectives set for all staff members contain sufficient risk and control objectives, alongside other role requirements or target business unit deliverables. Banks should ensure that there is a balance to ensure risk and compliance issues are targeted and measured where applicable.

6.1.3 The remuneration of non-executive directors, especially those who are members of board committees (for example audit or risk management committee) should take into account their responsibilities and time commitments, but should not be unduly related to the short-term performance of the bank.

6.1.4 It is recognised that in the Island the majority of banks are part of larger financial services groups and that remuneration and compensation packages for employees will often be based on a wider group approach.

7 Corporate structure, disclosure and transparency

7.1 *The board and senior management should understand the bank's operational structure and the risks that it poses*

7.1.1 The board and senior management should understand the structure and the organisation of the group of which the bank is a part, including the formal and informal links, relationships among relevant entities and with the parent. This should include understanding the legal and operational risks and constraints of the various types of intra-group exposures and transactions and how they affect the (subsidiary) bank's funding, liquidity, capital and risk profile under normal and adverse circumstances.

7.1.2 The (subsidiary) bank should have sound and effective measures and systems in place to facilitate exchange of information with relevant group entities and the parent to manage risks to which the bank may be exposed.

7.2 *The governance of the bank should be adequately transparent to its shareholders[4], depositors and other relevant stakeholders*

Transparency is essential for sound and effective corporate governance and its objective is to provide relevant parties with key information necessary to enable them to judge the effectiveness of the board and senior management.

It is recognised that transparency may be less detailed for non-listed banks, especially those that are wholly owned by their parent. However, these banks can

[4] In the Island the shareholder will normally be an intermediate or ultimate parent bank / financial services business.

pose risks to the financial system in the same manner as publicly quoted banks, including through participation in payments systems and, for Class 1(1) banks, the acceptance of retail deposits.

In addition to the regulatory requirements regarding the publication of annual financial statements which ensure disclosure of the bank's financial situation and performance (see Rule 2.22 / 2.24 of the Rule Book and associated guidance) a bank should, based on its size, complexity, ownership structure and risk profile, consider the disclosure of the following information:

- basic ownership structure (this is already covered for deposit advertising – refer to rule 6.16 of the Rule Book)
- governance codes / structures
- board structure
- board members' interests
- related party transactions

The disclosure of the above should be accurate, clear and presented in an understandable way, and can be made on the bank's website, in its annual financial statements or by other appropriate forms.

Appendix 1 – Glossary

"bank" is the Isle of Man incorporated deposit taker or the head office, or otherwise as applicable, of the branch.

"branch" means a branch in the Isle of Man of a deposit taker incorporated outside the Isle of Man.

Appendix 2 - Useful Website Links – further reading

Standard setting and professional bodies

ACCA: Association of Chartered Certified Accountants	www.acca.co.uk
BBA: British Bankers Association	www.bba.org.uk
BCBS: Basel Committee for Banking Supervision	www.bis.org
FRC: Financial Reporting Council *Combined Code – derived from the Cadbury and Greenbury Reports*	www.frc.org.uk
ICAEW: Institute of Chartered Accountants in England and Wales	www.icaew.com
ICSA: Institute of Chartered Secretaries and Administrators	www.icsa.org.uk
IoD: Institute of Directors	www.iod.com
OECD: Organisation for Economic Co-operation & Development	www.oecd.org

Reports on corporate governance

Walker Report: www.hm-treasury.gov.uk/walker_review_index.htm
(Recommendations on bank corporate governance)

The European Corporate Governance Institute has available on its site an Index of Codes page which includes the main reports on corporate governance published worldwide (listed by country). The UK list includes amongst other entries: www.ecgi.org

- Cadbury (1993 – financial aspects of corporate governance)
- Greenbury (1995 – remuneration)
- Hempel (1998 – review of Cadbury)
- Higgs (2003 – effectiveness of NEDs)