ISLE OF MAN
FINANCIAL SERVICES AUTHORITY

Lught-Reill Shirveishyn Argidoil Ellan Vannin

GUIDANCE NOTE FOR DEPOSIT TAKERS
(Class 1(1) and Class 1(2))

Operational Risk Management

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

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) or Class 1(2) regulated activity.

1.2 This guidance is designed to apply as widely as possible to assist banks in enhancing their operational risk management frameworks. It is intended to reinforce the key elements of widely accepted 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.

1.3 This should be read in conjunction with the guidance the Authority has issued to banks in relation to corporate governance but is intended to be more focussed on operational risk management. This guidance also links to sections in Part 8 of the Rule Book – Risk Management and Internal Controls, including specifically rule 8.6.

1.4 Effective operational risk 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 operational risk management including Sound Practices for the Management and Supervision of Operational Risk in 2003 and Principles for the Sound Management of Operational Risk in June 2011 which are accessible on its website www.bis.org.

1.5 Operational Risk is defined as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. Ordinarily it would include legal risk but would exclude strategic and reputational risk.

1.6 Rule 8.6 of the Rule Book requires banks to establish and maintain comprehensive policies appropriate to the nature and scale of business for managing certain risks, and review these policies at least annually. The risks mentioned include financial, legal, regulatory and other risks posed by a group company, which may affect the bank, and operational risks associated with the bank's activities.

1.7 Banks incorporated in the Isle of Man must hold capital in respect of operational risk. The capital charge has to be notified to the Authority in accordance with rule 8.48 of the Rule Book and reported on Form SR-1C, as at each quarter-end. The adequacy of the capital charge must also be considered in the ICAAP of those banks.

1.8 Standards of operational risk management in a bank may be relevant to the Authority's assessment of the competence of the directors and other responsible officers.

1.9 As operational risk continues to evolve the Authority expects banks to continuously improve their approaches to operational risk management.

2. Overview

2.1 Sound Operational risk management is a reflection of the effectiveness of the board and bank's management in administering its portfolio of products and activities.

2.2 Operational risk is potentially inherent in all banking products, activities, processes and systems, and the effective identification and management of it should be a core element of a bank's risk management programme.

2.3 Banks with a strong culture of risk management and ethical business practices are less likely to experience potentially damaging operational risk events and are better placed to deal effectively with those events that do occur.

2.4 Risk management in general encompasses the process of identifying risks to a bank, measuring the exposures to those risks (where possible) and ensuring that an effective capital planning and monitoring programme is in place.

2.5 Risk management procedures should include a sound internal control function and provide for the regular monitoring of any risk exposures and the corresponding capital needs on an ongoing basis; taking steps to control or mitigate any risks and the reporting of information to senior management and/or the board.

2.6 Operational risk management can vary from one institution to the next but common industry practice for risk governance often relies on three lines of defence being line management, an independent risk management function and a separate independent (typically an internal audit) review process.

2.6.1 The risk profile of a bank's activities will determine how this governance framework is implemented. This is an essential element in the safe and sound functioning of a bank and it may affect the risk profile if not implemented effectively. Business line management as the first line of defence is responsible for identifying and managing the risks inherent in the products, activities, processes and systems for which it is accountable.

2.6.2 The degree of independence of the risk management function, as the second line of defence, will differ among banks. For small banks, independence may be achieved through separation of duties and an independent review of processes and functions. In larger banks the operational risk function will have a reporting structure and will be responsible for reviewing and reporting through risk committees and compiling information for the senior management / board.

2.6.3 Internal audit coverage as the third line of defence should be adequate to independently verify that the risk structure is working as intended and is functioning effectively. People performing these reviews must be competent and appropriately trained and not involved in the development, implementation and operation of the risk management framework. Where audit activities are

outsourced, senior management should consider the effectiveness of the underlying arrangements.

2.7 Operational risk management is evolving and the business environment is constantly changing and management need to ensure that policies, processes and systems remain sufficiently robust. Improvements in operational risk management should be driven by experiences and management should be able to act promptly and appropriately on warnings received.

2.8 Sound operational risk management policies and procedures are essentially important in situations where a bank is experiencing problems or where significant corrective action is necessary.

2.9 A bank's operational risk governance should be fully integrated into the bank's overall risk management governance structure. In addition it is important that key personnel are fit and proper and suitably experienced for their jobs.

Local subsidiaries of international groups

2.10 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.

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

2.12 The specific guidance in sections 3 to 9 covers the relationship between a subsidiary and its group / parent in more detail where applicable.

Branches

2.13 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.

2.14 If the Isle of Man operation is a branch, then there should be documented delegated authority from the head office that provides senior management with the authority to operate and a framework in which this works.

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

- consider the standards and guidance referred to in sections 3 to 9, using its arrangements with the group to determine which of the functions are carried out by the local senior management and which are the responsibility of the head office;

- address the standards and guidance in sections 3 to 9 in ensuring that there is proper communication between the local senior management and head office; and

- branches in which the local senior managers delegate operational responsibility to other managers should consider the relevant standards and guidance on proper control by directors where they delegate (substituting local senior management for the directors).

Operational risk – fundamental principles and governance

3. Fundamental principles

3.1 ***The board of directors should take the lead in establishing a strong risk management culture. The board of directors and senior management should establish a corporate culture that is guided by strong risk management principles that supports and provides appropriate standards and incentives for professional and responsible behaviour.***

3.1.1 *Board responsibilities / corporate values*

Notwithstanding the requirements of section 6 of the Rule Book to observe high standards of integrity the board should set out an appropriate code of conduct and oversee the implementation of appropriate ethical values, principles and values, and ensure all staff understand their roles and responsibilities.

Any code of conduct should be aligned to the bank's statement of risk appetite and tolerance

3.1.2 *Training*

An appropriate level of operational risk training should be available at all levels throughout the organisation. The training should appropriately reflect the roles and responsibilities of the individuals for whom it is intended and who have to perform the tasks.

3.2 ***Banks should develop, implement and maintain a risk management framework that is fully integrated into the bank's overall operational processes. The framework for operational risk management will depend on a range of factors, including its nature, size, complexity and risk profile.***

3.2.1 The board and bank management should ensure it understands and recognises the nature and complexity of the all risks inherent in the business and review these on a regular basis.

3.2.2 The means of understanding the nature and complexity of operational risk is to have a framework to consider all business lines, new business initiatives, products, systems and processes across all levels of the bank and the risks that may accrue

from these. This should link to the risk appetite of the bank (see section 4.2). The framework should be comprehensively documented in board approved policies and should include definitions of operational risk and loss events.

The framework documentation should include:

a) an organisational structure setting out reporting lines, individuals' responsibilities and accountabilities;

b) information of any risk assessment tools and how they are used;

c) an outline of the bank's operational risk appetite and tolerance, as well as the thresholds or limits for inherent and residual risk, and any risk mitigation mechanisms and strategies;

d) how the bank establishes and monitors limits for inherent and any residual risk exposure;

e) the management information that can be produced to aid the monitoring and risk reporting;

f) a definition of operational risk to ensure there is consistency in the risk identification, and risk management objectives;

g) details of any independent review and assurance procedures for operational risk processes; and

h) circumstances that would require the operational risk policies to be reviewed (such as a material event or change in the risk profile of the bank).

4. Governance – the Board of Directors

This section should be read in conjunction with the more comprehensive corporate governance guidance note for banks the Authority has issued. The following is only intended to focus on the specific governance of operational risk management.

4.1 ***The board of directors should approve and periodically review the risk management framework and oversee senior management to ensure that the policies, processes and systems are implemented at all decision levels.***

4.1.1 The board of directors should:

(a) establish the management culture, and supporting processes, and understand the nature and scope of the operational risks inherent in the bank's strategies and activities;

(b) set clear lines of responsibility and accountability for senior management which define the control functions and expectations and approve the corresponding policies developed by senior management;

(c) regularly review the framework to ensure that the bank has identified and is managing the operational risks arising from external market changes and other environmental factors, as well as any operational risks associated with new products, activities, processes or systems, including changes in risk profiles and priorities (e.g. changing business volumes);

(d) ensure that the bank's framework is subject to effective independent review by audit or other appropriately trained parties; and

(e) ensure that if there are any material events or best practice points that affect the risk profile of the bank these are accommodated within policies and procedures.

4.1.2 The board of directors should establish clear lines of management responsibility and accountability for implementing a strong control environment. The control environment should provide appropriate independence / separation of duties between operational risk management functions, business lines and support functions.

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

4.1.4 The board should ensure that the control functions are properly staffed and resourced so that staff can carry out their responsibilities independently and effectively.

4.2 ***The board of directors should approve and review a risk appetite and tolerance statement for operational risk that articulates the nature, types and the levels of operational risk that the bank is willing to assume.***

4.2.1 When considering or approving the appetite and tolerance for risk the board should take all relevant risks and the bank's strategic direction into account. This may include any changes in the external environment. This should be reviewed at least annually and include appropriate thresholds or limits for specific loss events.

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

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

4.3.2 It is expected that a subsidiary bank in the Isle of Man will be subject to oversight by the parent / group. The local management and board should however have appropriate input into any local or regional adoption of risk methodologies and to assessments of local risks.

4.3.3 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.

The subsidiary (local) board should retain and set its own operational risk 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.

4.3.4 *Business line and matrix management*

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

The board and senior management should ensure that the decisions of matrix and business line management structures do not affect the operational risk framework. Information should be consolidated centrally and be consistent in approach.

4.3.5 *Outsourcing of key risk functions*

Whilst the Authority allows the outsourcing of processes or activities to third parties (rule 8.16) this does not transfer the responsibility to those third parties. The Authority's consent is required where a material function is to be outsourced and if a bank is in any doubt as to what this means the Authority should be contacted for clarification.

While outsourcing can help manage costs, provide expertise, expand product offerings, and improve services, it also introduces risks that management should consider and address. The board and senior management are responsible for understanding the operational risks associated with any outsourced arrangements and ensuring that effective risk management policies and practices are in place to manage the risk in respect of outsourcing activities.

Where a bank is proposing to carry out any outsourcing it should undertake appropriate due diligence to confirm the standing of the proposed provider. The consent of the Authority is required for any material function that is outsourced.

5. Governance - Senior Management

5.1 ***Senior management should develop for approval by the board a clear, effective and robust risk management structure which is well defined, transparent and with consistent lines of responsibility. It should be senior managers' responsibility for managing the operational risk and ensuring that policies and procedures are consistently applied.***

5.1.1 Senior management should assist with the development and implementation of the operational risk management framework including the development of policies and procedures.

5.1.2 The risk management function should be responsible for identifying, measuring, monitoring, controlling or mitigating, and reporting on risk exposures. Senior management should ensure that staff responsible for implementing and managing operational risk understand and prepare any reports consistent with the risk appetite of the bank.

5.1.3 All staff responsible for managing and controlling operational risk within business units should have clear objectives and accountability. They should also be able to coordinate and communicate effectively with other staff involved with the business.

5.1.4 Staff responsible for monitoring and enforcing compliance of the bank's procedures / risk policy should have a separate reporting line, independent from the units they oversee (if possible). It is recognised that it is not uncommon for risk managers to work closely with individual business units and to have dual reporting lines.

5.1.5 Staff directly involved with the evaluation of operational risk reviews should be independent of the business unit they oversee and have the necessary experience, technical capabilities and access to all information. The risk review function should be adequately resourced both from a systems and staffing perspective (including personnel who possess sufficient experience, knowledge and qualifications where appropriate).

5.1.6 It is sound industry practice for banks to have an operational risk committee or a risk committee that is made up from members of staff with expertise in business activities, finance or risk management.

The risk committee's mandate, reporting lines, composition and working procedures should be well defined. It should have an adequate and appropriate composition of experience and be subject to an independent challenge or verification and validation process.

In cases where members provide input it should be considered if they have any conflict of interest in respect of the information they present.

5.1.7 Committee meetings should be held at appropriate frequencies with adequate time and resources to permit productive discussion and decision-making. Records of committee operations should be adequate to permit review and evaluation of the committee effectiveness.

5.1.8 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' line management.

Risk Management Environment

6. Identification and Assessment

6.1 ***Senior management should ensure the identification and assessment of the operational risk inherent in all material products, activities, processes and systems are well understood, taking into account inherent risks and incentives.***

6.1.1 Sound risk assessment assists a bank in understanding its risk profile and allows it to target its risk resources and strategies most effectively.

6.1.2 Senior management should ensure that the identification and assessment of the operational risk, inherent in all material products, activities, processes and systems is fully understood. This should take account of both internal and external factors and could include for example the bank's structure, the nature of the bank's activities, the quality of the bank's staffing resource, any organisational changes and employee turnover.

6.1.3 Examples of tools that may be used for identifying and assessing operational risk may include:

(a) Internal / External Audit Findings: while audit findings primarily focus on control weaknesses and vulnerabilities, they can also provide insight into some potential inherent risks.

(b) Typologies / loss data: analysis of actual loss events or industry experiences can provide an insight into the actual causes of losses, any failings of internal controls and any systematic occurrences outside the control of the bank. This information can be used to explore possible weaknesses in the bank's control environment and enable it to consider previously unidentified risk exposures.

(c) Loss events connected to credit and market risk may relate to operational issues and should be segmented in order to obtain a more complete view of the operational risk exposure.

(d) A risk (control) self assessment process can be a useful tool to assess the underlying risks against a library of potential threats and vulnerabilities captured on a risk register and regularly reviewed. This can typically evaluate inherent risk

(the risk before controls are considered), the effectiveness of the control environment, and residual risk (the risk exposure after controls are considered).

(e) Business process mappings: these help identify the key steps in business processes, activities and organisational functions. Process maps can reveal individual risks, risk interdependencies, and areas of control or risk management weakness. They also can help prioritise subsequent management action.

(f) Risk and performance indicators such as Key Risk Indicators ("KRIs") provide an insight into a bank's developing risk exposure. KRIs can provide insight into the status of operational processes, which may in turn provide insight into operational weaknesses, failures, and potential loss. Risk and performance indicators are often used with triggers to warn when risk levels exceed acceptable ranges and prompt mitigation plans.

(g) External review / expert opinion of business line and risk managers can identify potential operational risk events and assess the potential outcome. This type of scenario analysis is an effective tool when considering potential sources of significant operational risk and the need for additional risk management controls or mitigation solutions.

6.2 ***Senior management should ensure that there is an approval process for all new products, activities, processes and systems that fully assesses operational risk.*** *(Rule 8.13 also refers)*

6.2.1 A bank's operational risk exposure can increase when it is engaged in any new activity, launches a new product, enters new or unfamiliar markets, implements any new business processes or changes its computer systems. The risk can also increase where businesses are distant from the head office. The level of risk may escalate if the introduction of any new event represents a material source of revenue or is a business-critical operation.

A bank should ensure that its risk management controls take into account any changes to products, activities or systems.

6.2.2 A bank should have policies and procedures that address the process for review and approval of new products, activities, processes and systems.

The review and approval process should consider:

(a) any inherent risks in the new product, service, or activity (*the Authority's guidance note on advertising sets out the expectations in relation to the promotion of any new deposit products)*;

(b) any changes to the bank's operational risk profile, risk appetite and risk tolerance, including the impact on existing products or activities;

(c) the necessary controls, risk management processes, and risk mitigation strategies;

(d) any residual risk; and

(e) the procedures to measure, monitor, and manage the risk of the new product or activity.

6.2.3 The approval process for new products, processes and systems should include an assessment of the impact on the business and customers. It should also consider whether an allowance for any additional staffing is required and the impact of any technology issues before being introduced.

The implementation of new products, activities, processes and systems should be monitored in order to identify and address any material issues.

6.2.4 Business activities can become misaligned with risk management when the price of risk is not understood and considered in the pricing of products, the measurement of risk exposure, and the cost of risk management.

7. Monitoring and Reporting

7.1 ***Senior management should implement a process to regularly monitor and review operational risk profiles and material exposure to losses. Appropriate reporting mechanisms should be in place at the board, senior management and business line levels that support proactive management of operational risk.***

7.1.1 Information to monitor risk reporting should be comprehensive, accurate, consistent and actionable across business lines and products. Reports should however also be manageable in scope and volume.

7.1.2 Information should be communicated in a timely and understandable manner to enable management 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.

7.1.3 The results of the monitoring activities across individual business / portfolio risks should be included in regular management and board reports.

7.1.4 Consideration of the bank's current and potential operational risk exposures would also assist in determining if any additional capital is required to cover inherent risk in the ICAAP. Market conditions and trends should be taken into account where applicable.

7.1.5 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.

7.1.6 Operational risk reports may contain internal financial, operational, and compliance indicators, as well as external market or environmental information

about events and conditions that are relevant to decision making. Operational risk reports should include:

(a) details of numbers and trends;

(b) any breaches of the bank's risk appetite and tolerance statement;

(c) details of any significant internal operational risk events and losses; and

(d) any relevant external events and the potential impact on the bank and operational risk capital.

Data capture and risk reporting processes should be analysed periodically with a view to continuously enhancing risk management.

8. Control & Mitigation

8.1 ***Banks should have a strong control environment that uses policies, processes and systems; appropriate internal controls and appropriate risk mitigation and/or transfer strategies.***

8.1.1 Internal controls are intended to provide reasonable assurance that key risks to the business are mitigated by appropriate oversight. Any such process or measure, if applied properly, safeguards assets, produces reliable financial reports and ensures compliance with applicable laws and regulations.

Internal controls help avoid actions being taken beyond the authority of an individual, mitigate fraud and place checks on discretions. Even in very small banks key management decisions should be taken by more than one person.

8.1.2 A sound internal control programme consists of five components that are integral to the risk management process: control environment, risk assessment, control activities, information and communication, and monitoring activities. This includes reviews against stated objectives, verifying compliance with management controls, reviewing the treatment and resolution of cases of non-compliance, considering the levels of authorisation that apply and tracking any management overrides or deviations from policies.

8.1.3 An effective control environment also requires appropriate segregation of duties although in some smaller banks this is sometimes more difficult to achieve. Assignments that establish conflicting duties for individuals or a team without dual controls or other countermeasures may enable concealment of losses, errors or other inappropriate actions.

Any areas of potential conflicts of interest should be identified, minimised, and be subject to careful independent monitoring and review. Where any conflicts are

identified these should be recorded in the conflicts register and reviewed periodically, at least annually, by the board.

8.1.4 In addition to considering the segregation of duties and dual control, banks should ensure that there are other appropriate internal controls to mitigate operational risk. This could include:

(a) clear authorities and/or processes for approval and how any departure to policy is managed;

(b) monitoring of adherence to assigned risk limits or thresholds;

(c) the safeguards for access to, and use of, bank assets and records;

(d) the required staffing level and training to maintain expertise;

(e) the ongoing processes to identify business lines or products where returns appear to be out of line with reasonable expectations;

(f) regular verification and reconciliation of transactions and accounts; and

(g) a staff policy that provides for officers and employees being obliged to take holiday absence for a period of at least two consecutive weeks in any one year.

8.1.5 Management should ensure the bank has a sound Information Technology ("IT") infrastructure that meets current and long-term business requirements by providing sufficient capacity for normal activity levels as well as peaks during periods of market stress; ensuring data and system integrity, security, and availability; and supporting integrated and comprehensive risk management.

8.1.6 IT can be used to aid the control environment as automated processes are less prone to error than manually completed tasks. However, automated processes introduce other IT risks that must also be addressed through appropriate risk management programmes.

8.1.7 The use of technology related products, delivery channels and processes exposes a bank to strategic, operational, and reputational risks and the possibility of material financial loss. Consequently, a bank should have an integrated approach to identifying, measuring, monitoring and managing any technology risks.

8.1.8 Sound technology risk management uses the same precepts as operational risk management and requires:

(a) governance and oversight controls that ensure IT, including outsourcing arrangements, is aligned with and supportive of the bank's business objectives;

(b) policies and procedures that facilitate the identification and assessment of risk;

(c) establishment of risk tolerances and performance expectations to assist in controlling and managing risk; and

(d) implementation of an effective control environment and the use of risk transfer strategies that mitigate risk; and monitoring processes that test for compliance with policy thresholds.

8.1.9 *Mergers and acquisitions*

Mergers and acquisitions can result in fragmented infrastructure and cost-cutting measures or inadequate investment and can undermine a bank's ability to aggregate and analyse information across risk dimensions or manage and report risk on a business line or legal entity basis.

Management should ensure appropriate arrangements are in place to provide for a robust infrastructure at all times, particularly before mergers / integrations are agreed or new products are introduced.

8.2 *Internal / External Audit function*

8.2.1 It is good practice for all banks to consider their susceptibility to internal and external fraud and have an internal audit function that can provide an independent review and challenge or verification and validation of the bank's operational risk management controls, processes and systems.

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.

8.2.2 The internal audit coverage should be adequate to independently verify that the risk framework has been implemented as intended and is functioning effectively. Where audit activities are outsourced, senior management should consider the effectiveness of the underlying arrangements and the suitability of relying on an outsourced audit function as the third line of defence.

8.2.3 Internal audit coverage should include opining on the overall appropriateness and adequacy of the operational risk management framework. Internal audit should not only be testing for compliance with approved policies and procedures, but should also be considering if the risk framework meets all organisational needs.

9. Business Resumption, Continuity and Contingency

9.1 ***Banks should have business resumption, continuity and contingency plans in place (as required by rules 8.14 and 8.15) to ensure an ability to operate on an ongoing basis and limit losses in the event of severe business disruption.***

9.1.1 Business resumption, continuity and contingency arrangements should be commensurate with the nature, size and complexity of the bank's operations. Plans should take into account different types of likely or plausible scenarios to which the bank may be vulnerable and the operational risk issues that may arise from these. Such incidents that damage or make inaccessible the bank's facilities, IT infrastructures, or events that can create a human resources issue could result in significant losses to the bank.

9.1.2 Plans should incorporate a business impact analysis, recovery strategies, testing, training and awareness programmes, lines of communication and crisis management programmes. A bank should identify critical business operations, key internal and external dependencies, and resilience levels.

9.1.3 Continuity plans should establish contingency strategies, recovery and resumption procedures, and communication plans for informing management, employees, the Authority, other relevant regulatory authorities, customers, suppliers and where appropriate other agencies.

9.1.4 Plans should be reviewed and tested periodically to ensure they remain consistent with current risks, threats and recovery priorities. Appropriate training and awareness programmes should also be implemented to ensure staff can effectively execute contingency plans. The testing should aim to ensure that recovery and resumption objectives and timeframes can be met, and a full scenario test can help with analysing the robustness of the arrangements internally and with key service providers. The results of testing should be reported to the management and board.

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 – Acknowledgements and further reading

BCBS: Basel Committee for Banking Supervision	**www.bis.org**
Building a framework for operational risk management	**www.bankofengland.co.uk**
British Bankers Association	**www.bba.org.uk**
Financial Stability Institute	**www.fsiconnect.org**
IoD: Institute of Directors	**www.iod.com**