Business Continuity Planning and Disaster Recovery Management in the Banking Sector of the Bailiwick of Guernsey

A Thematic Report issued by the Guernsey Financial Services Commission

October 2008

Table of contents

1 Executive summary

- In general, business continuity planning and disaster recovery management is of a satisfactory standard across the industry with a small number of exceptions to good practice that have been addressed with the banks visited by the Commission.
- The exceptions included an insufficiently wide scope for business continuity plans, absence of an up to date business impact analysis and relevant list of business recovery priorities, insufficient testing of call trees, and a lack of a secondary muster point for staff.
- A number of areas of good practice were observed including active monitoring by one bank of both actual and potential events that could invoke its plan, and the use of brightly colour role-specific cards and contact lists that could by picked up easily by key personnel in an emergency.
- One island-wide risk emerged from the review that concerns all businesses in Guernsey, and that is the concentration risk associated with the limited availability of disaster recovery service providers and resources. The industry is requested to address this risk more thoroughly.

2 Introduction and methodology

2.1 Introduction

As an integral part of its on-going supervision of licensed banks, the Guernsey Financial Services Commission ("the Commission") carried out a review of business continuity planning and disaster recovery management as a key element of the operational risk faced by the banking industry in the Bailiwick of Guernsey. The Commission is committed to ensuring the compliance of the Guernsey banking industry with The Core Principles for Effective Banking Supervision. Core Principle 15 "Operational risk", essential criteria 4 states:

> *"The supervisor reviews the quality and comprehensiveness of the bank's business resumption and contingency plans to satisfy itself that the bank is able to operate as a going concern and minimise losses, including those that may arise from disturbances to payment and settlement systems, in the event of severe business disruption."*

The aim of the review was to confirm whether banks have locally relevant, up-to-date, and regularly tested business continuity and disaster recovery plans, in order to assess whether there were significant gaps or exceptions to best practice that could set operational risk levels at a level that was unacceptable for the Commission. Unexpected operational disruptions to banking operations can have a substantial adverse impact on day-to-day business objectives as well as seriously damaging the wider societal roles played by banks. The Commission therefore attaches the highest importance to banks having in place proportional, relevant and practical plans to mitigate the probability of impact of such operational disruptions.

The purpose of this thematic report is to summarise the key findings of the Commission's review in order to improve risk management practice in relation to business continuity and disaster recovery and to ensure that the local banking industry is prepared to respond adequately to any major operational disruptions. The report is not intended to give a comprehensive description of all risks faced by Guernsey banks that relate to major operational disruptions, nor do the findings cited in the report represent issues faced by all

banks. Rather the report is intended to highlight both weaknesses and good practice in business continuity planning and to devise measures and supervisory responses to any issues identified.

It is the Commission's intention that business continuity and disaster recovery plans will be regularly reviewed as part of the on-site visits programme in order to ensure the industry is keeping pace with the changing environment and risk profiles of the businesses, as well as to follow up on any recommendations made to individual banks.

2.2 Methodology

The Commission's thematic review was based on the 'High Level Principles for Business Continuity' paper published by the Joint Forum of the Basel Committee on Banking Supervision, International Organisation of Securities Commissions and the International Association of Insurance Supervisors. This paper sets out expectations of good practice in the following areas:

- Board / Management responsibility;
- Major operational disruptions;
- Recovery objectives;
- Communications;
- Cross-border communications;
- Testing.

The thematic review took place in two stages. Stage 1 was completed by the middle of May 2008 and included an industry wide survey with key questions on good practice in business continuity management.

Stage 2 involved on-site visits to a selection of banks and was completed by the end of July 2008. In selecting the licensees for the on-site visits programme, the Commission chose a diversified sample of banks on the island (e.g. clearing banks, private banks, deposit takers, subsidiaries and branches.) as well as considering individual responses to the industry-wide survey. The Commission conducted five on-site visits in total during which it reviewed in detail the banks' policies, procedures and documentation in relation to their business continuity planning and disaster recovery management. The Commission also assessed documentary evidence relating to the key building blocks of any business continuity and disaster recovery plan, which are

- business impact analysis - identifying critical operations, services, establishing clear communication protocols (both internal and external) and setting appropriate resilience levels;
- identification of recovery objectives and prioritisation of these based on the business impact analysis;
- business continuity plans laying out the detailed guidance for implementation of the business continuity and disaster recovery strategy defined by the business impact analysis and the recovery objectives.

Prior to the commencement of the thematic review the Commission identified three risks that had special relevance for the banking sector in Guernsey:

- the concentration risk due to the limited availability of disaster recovery service providers and resources on the island;

- the risk of insufficient local management involvement in business continuity planning, an overreliance on group policies and manuals, and a lack of consideration for Guernsey specific factors. These risks may arise from the fact that all banking licensees in Guernsey are branches or subsidiaries of banks in other jurisdictions.
- insufficient or irregular staff training and involvement in the business continuity and disaster recovery process, due to the mobility of the labour pool on the island.

The Commission's findings in respect of these three key risks are set out in Section 3.

3 Findings

3.1 Overview

The results of the review suggested significant gaps or exceptions to best practice were rare. The majority of business continuity plans were up-dated and tested annually, with senior management involved in the planning process. Some policy and procedure exceptions were identified by the Commission during the on-site visits and are being rectified by the banks concerned. There were also several examples of good practice encountered during the on-site visits.

None of the banks visited had invoked their business continuity plans, although one bank had been a recovery site for a Group entity in the Cayman Islands that had been forced to invoke its plan when Hurricane Ivan struck the area in 2005.

Of the three potential key risks examined during the review, only one, the concentration risk due to the limited availability of disaster recovery service providers and resources was present, and this is dealt with in Section 3.4. The Commission found no evidence that local senior management were not engaged in business continuity planning, or that the "local" angle was missing from plans. Not all banks visited had the benefit of a comprehensive Group business continuity policy on which to base their plans, but the Commission found examples of good practice amongst those who had developed their own plans. In terms of staff training, the Commission found no evidence that staff were untrained or disengaged from the business continuity process, and examples of good practice in this area were encountered.

3.2 Findings from the industry wide survey

The initial industry-wide survey painted a generally positive picture of business continuity planning and practice across the banking sector in the Bailiwick. Where responses received appeared to be unusual (such as the bank that responded to Question 3 of the survey that it had never tested its business continuity plan for example), these banks were selected for an on-site visit. The results of the industry-wide survey are summarised below:

1. Has a formal Business Continuity and Disaster Recovery Plan been approved by the senior management or the Board of Directors of the bank?	For 96% of the licensees the Board / senior management formally approved the plans. The remaining 4% responded that their business continuity plans were under review and would be formally approved once the review was complete.

2. What is the date the plan was last up-dated?	The majority of licensees had updated their plans in 2008 with 66% or 31 licensees having done so in the first four months of 2008. For 32%, or 15 licensees, the last update was in 2007 and only 1 licensee replied that its plan was last updated more than two years ago.
3. What is the date the plan was last tested and what were the results of the test?	The majority of license holders tested their plans and procedures in 2007 – 70%, while 17% did testing in 2008. 6% of the banks tested their plans for the last time in 2006 and only 1 of the banks replied that they had never tested their business continuity and disaster recovery plan.
4. Is business continuity and disaster recovery management included in the bank's annual budget?	70% of the banks had a dedicated budget for business continuity and disaster recovery, whilst the remaining 30% had no dedicated budget, but made provision for a business continuity element in other budgets, such as IT for example.
5. Has business continuity and disaster recovery been subject to independent review?	64% of the banks confirmed that their policies and procedures had been reviewed by independent third parties. These included group internal auditors, security, IT or risk departments.
6. Are specialist services providers used for business recovery and disaster recovery management?	60% of the banks used the services of specialist service providers. These include provision of back-up and recovery sites, logistics support, advice on preparation, up-date and testing of business continuity plans. 40% of the licensees relied on their own resources and did not use any external service providers.
7. What is the location of disaster recovery site(s)?	There is a relatively well diversified positioning of the disaster recovery sites on Guernsey and in some cases, other locations such as Jersey or the UK. However three geographical locations on Guernsey provide the business continuity sites for 30 of the licensees (64% of all licensees). The point is dealt with further in Section 3.4 of this report.

The results revealed a number of areas of good practice:

- **Regular updating of business continuity plans**. Good practice would be to consider the plan as a living document to be updated annually or sooner if there is a change in the business, key personnel, premises, etc.

- **Budgeting for business continuity planning and disaster recovery management**. The Commission is aware that practice across industry in general varies between having a dedicated budget and making provision within other budgets, such as IT services or premises for example, for a business continuity element. Both of these are acceptable.

- **Review of the business continuity plan by an independent third party.** The Commission would strongly encourage banks to have their plan reviewed by an independent third party (which could be a group resource) to ensure that it is appropriate for the size and nature of the business and to ensure that all "gaps" are covered.

3.3 Entity-specific findings from the on-site visits

3.3a Exceptions

The following exceptions to good practice were identified in relation to business continuity planning and disaster recovery management for four of the five banks visited, and an exceptions letter was issued to each bank concerned requiring it to address the issues within a defined timescale.

It is the Commission's view/expectation that senior management of all banks in the Bailiwick who read this report and identify any of the issues described below as being applicable to their own bank's business continuity plan, will wish to take steps for business reasons to rectify such exceptions in order to minimise the operational risk to which the bank is exposed.

Scope of business continuity plans
Scope of the plan is important in determining whether a business has an effective business continuity solution that can rapidly substitute crucial resources or redirect work elsewhere. If the scope is too narrow, a perfectly functioning plan in one scenario may fail completely in another.

A common theme observed during the visits was that some business continuity plans were too narrow in scope in terms of the type of business disruption, rather than the cause, that the bank expected to encounter. Examples of this narrow focus included:

- plans that considered how a business would respond to an event happening out of working hours, but did not detail what would happen if a major business interruption occurred during business hours.

- plans that defined a major business interruption as one in which the bank's building was inaccessible, but did not adequately consider events that might have a detrimental impact on business whilst leaving the building unaffected. A pandemic was commonly mentioned, but there are other events in this category such as an industry-wide failure in payment systems, an ongoing UK postal strike or a sudden loss of skilled staff that should be considered for relevance.

- plans that did not consider how the bank might respond to localised events that may prevent the use of both the bank's main site and its disaster recovery site. The assumption made by some banks visited was that an event disabling both their primary and alternate site could only be catastrophic for Guernsey (a meltdown at the nuclear power plant at Cap De La Hague for example) and it was pointless therefore to consider it from a business continuity and disaster recovery perspective. However, there could be a number of events that may render both a primary and an alternate site for a specific bank useless without being a full-scale catastrophe, such as a power failure in one or more parishes for example. Banks need to give adequate

consideration to such events in their business continuity and disaster recovery planning.

Business impact analysis

A business impact analysis takes each part of each operation and considers what the impact on the business will be if that task is not recovered over a range of timescales such as an hour, a day, a week, etc. From this, the list of recovery priorities and timescales and the communications strategy can be generated. The analysis should be updated as the business changes and reviewed regularly.

It is an essential part of business continuity planning, but some of the banks visited either did not have a business impact analysis or had one that was no longer relevant.

Recovery objectives

A necessary part of every business continuity plan is a list of recovery objectives detailing which operations are to be recovered first, to what level, over what timescale and with what minimum number of critical staff. The list should be driven from the outcome of the business impact analysis and should be part of the plan document.

Not every bank visited had a list of recovery objectives.

Testing of the business continuity plan and the call tree

Regular testing of the plan is an essential tool to ensure that staff understand the plan and their roles within it. Whilst there was no evidence to suggest that testing, either through a full scenario-type test, an IT systems test or a walkthrough with staff of the plan page by page, was not being carried out regularly, not all banks were formally recording testing events or their outcomes. As a result, this information was not being fed back into the Group operational risk framework.

A number of banks had call trees in place but had not tested them because they were confident that staff contact numbers were accurate. Given that the call tree is essential to the early success of a business continuity plan's invocation, it should be tested regularly. This will not only flush out inaccurate contact details, but will also ensure that when the correct number is called, there is no unexpected impediment to making contact with the member of staff, such as a fax phone left permanently on fax, or a member of the household who is unwilling to pass on a message.

Outsourcing to Group or external parties

Two of the banks visited relied on other entities within their banking Group to carry out key functions for them, such as payments, settlements or investment management advice, such that the unavailability of these functions would have a major impact on the business of the Guernsey bank. However, neither of these banks was aware of the business continuity and disaster recovery arrangements for the site(s) on which they relied, or the anticipated recovery times for those sites. In both cases, this exception has already been rectified.

The principle can be extended to any supplier of key services, including those involved in IT and disaster recovery support in the event of a crisis. The Commission would expect banks to have a Service Level Agreement with all key internal or external suppliers and to be aware of the Business Continuity arrangements of any supplier, including intra-Group relationships. This awareness should extend to the estimated recovery times for those suppliers. A bank should also ensure that the business continuity and disaster recovery arrangements of the suppliers on whom it relies fall within the bank's risk appetite. Adequate contingency planning should be in place in case the service provider is unable to deliver critical services to the Guernsey bank.

Alternate muster point
One reason for the failure of business continuity plans is that the muster point for staff is so close to the primary site that it too becomes inaccessible in the event of a major disaster, and staff therefore have no other pre-determined place in which to assemble. Wherever practicable, banks should consider introducing a second muster point, preferably in the opposite direction to the first point and some further distance away, to which staff could go. Alternatively, the plan could direct staff to go straight home in the event that the primary muster point is unavailable.

3.3b Good practice

The Commission observed a number of areas of good practice during the visits:

- One bank used a simple spreadsheet to record events that had the potential to impact on the bank's business continuity plan. This list included local events that had occurred but had not invoked the plan, such as a small fire on the premises, and wider scale events such as an industry-wide CHAPS failure that, had it been of a longer duration, would have impacted on this particular bank's business. The list was used to inform the business impact analysis to ensure that the scope of the current plan did not contain significant "gaps".

- One bank, that did not have the benefit of a comprehensive and benchmarked Group business continuity policy, had purchased software to benchmark its own plan against BS25999, the British Standard for business continuity management.

- One bank used brightly coloured laminated "role cards" detailing the specific tasks and contact lists for each member of its Emergency Management Team to follow in the event of a disaster. These roles were also set out in the plan itself, but separating each one onto a brightly coloured card provided a tightly focussed and easily recognised aide memoir for each key person.

- One bank kept a copy of its plan on a clip-board by the exit so that it could be grabbed quickly, along with a roll call list, in the event of the building having to be evacuated.

- In addition to business continuity training, one bank with a small number of staff had put all personnel through first aid and fire safety training, in order to increase their confidence in dealing with an emergency situation.

- All banks visited had a range of mobile phones, Blackberrys and land lines from more than one telecommunications provider, so that in the event of a primary failure of one of those providers, contact with Group and external parties could still be maintained.

- All banks visited had measures in place within the business continuity plan to secure the building immediately if it had to be evacuated, in order that confidential documents, data and valuables could not be accessed by the public. A number of the banks also used document scanning systems, so that crucial documents could be available electronically at their alternate site.

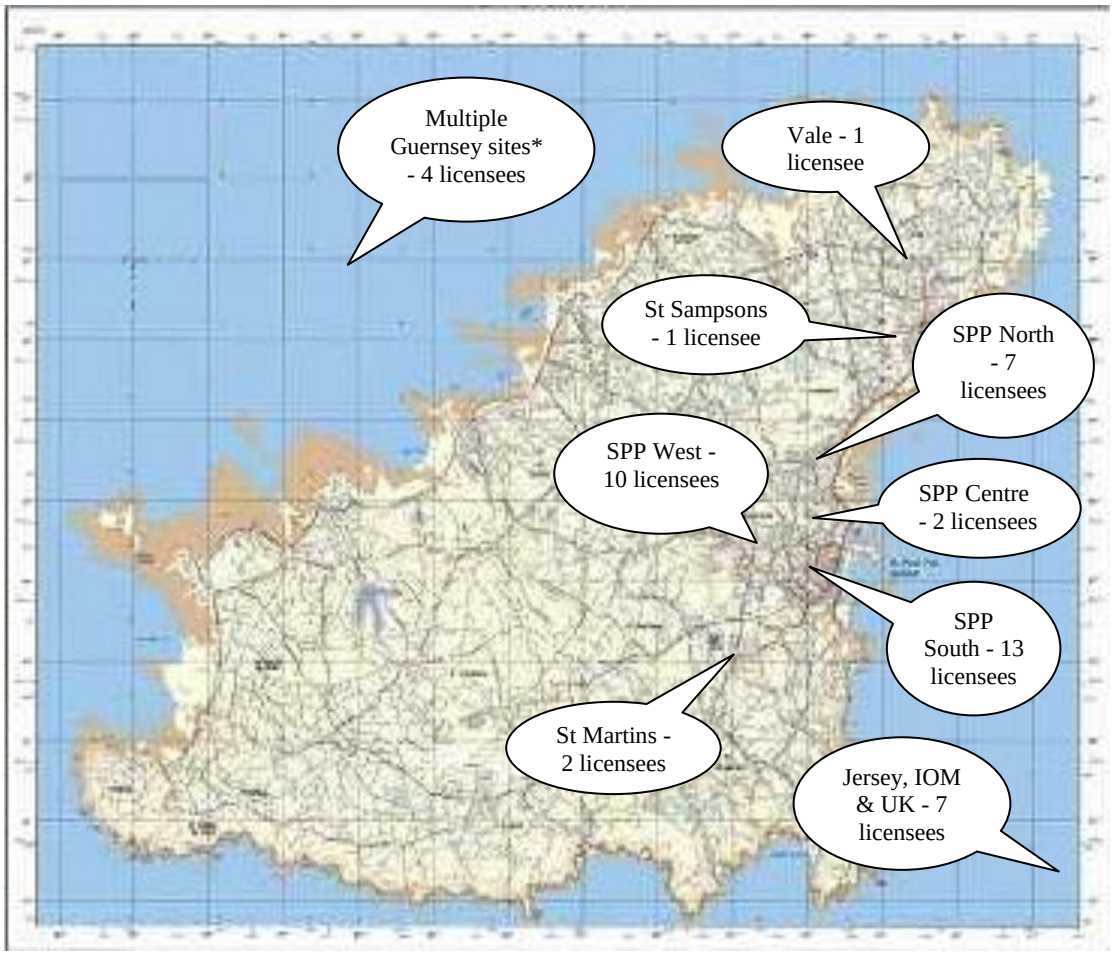
- A number of banks had established a dedicated phone line for staff to contact in an emergency in order to get the latest update on the situation via recorded messages.

3.4 Island-wide concerns

Concentration risk – disaster recovery service providers

One of the key risks considered by the Commission during the review was whether there was a concentration risk in the use of disaster recovery sites or personnel. Given the size of Guernsey this is almost inevitable and Question 7 of the survey was designed to assess how great the concentration risk was.

Below is a map of Guernsey with the concentration of disaster recovery sites for Guernsey banks highlighted.



* a choice of branch/retail locations in Guernsey

It is not surprising that the majority of recovery sites (the sites of 32 licensees) are located within the borders of St Peter Port (being the main business area of the island). Some of these sites are operated exclusively for the bank in question, but 17 of the 32 sites in the St Peter Port area are operated by three disaster recovery service providers.

There are two different concentration risks here. The first is geographical in that an event affecting the east of the island or the St Peter Port area specifically, could disable 68% of the alternate sites for the Guernsey banking industry (and in the vast majority of cases, the primary site too).

The second risk involves the concentration of businesses using third party service providers, either to provide physical space for disaster recovery, or IT recovery support, or both. When the number of non-banking businesses also using these facilities is taken into account, the concentration risk in the event of a major business interruption affecting many organisations is considerable.

During the course of the on-site visits, a number of banks explained that some or all of their operations could be switched to other group entities in the event that access to both the primary and alternate site on Guernsey was compromised. The concentration risk is therefore mitigated to some extent by these arrangements and the Commission would encourage banks to have an off-island "back-up plan" to mitigate the concentration risks outlined above.

Despite the mitigation represented by the off-island contingency arrangements in place for some banks, the Commission considers the concentration risks for the banking sector in Guernsey to be considerable. It has therefore asked the Association of Guernsey Banks to consider the business implications of the risks outlined above and suggest what action might be taken to reduce the risk.

4 Acknowledgements

The Commission would like to thank banking licensees in Guernsey for contributing to the island-wide survey, and for participating in the on-site visits where selected to do so.

5 Useful websites

UK Financial Sector Continuity
Established by the UK's Tripartite Authorities (HM Treasury, the Bank of England and the Financial Services Authority) to provide a central point of information about work on continuity planning that is relevant to the UK's financial sector.
www.fsc.gov.uk

Financial Services Authority (FSA)
The UK regulator's "Business Continuity Practice Management Guide"
http://www.fsa.gov.uk/pubs/other/bcm_guide.pdf

Basel Committee on Banking Supervision
The "High Level Principles for Business Continuity" document.
http://www.bis.org/publ/joint14.pdf

The Business Continuity Institute (BCI)
The BCI was established in 1994 to enable individual members to obtain guidance and support from fellow business continuity practitioners. The BCI currently has over 4000 members in 85+ countries. The BCI Good Practice Guide can be downloaded from this website.
www.bci.org

The Institute of Operational Risk (IOR)
The Institute of Operational Risk was created in January 2004 as a professional body to establish and maintain standards of professional competency in the discipline of Operational Risk Management.
www.ior-institute.org

Disclaimer

The foregoing is not intended as formal regulatory guidance, nor should it be taken to cover all relevant aspects of the subjects touched upon. Rather, it highlights shortcomings identified which, if addressed at an early stage, may help mitigate risk levels and avoid specific pitfalls.