

Business Continuity

FSA Guidance

Antony Davies

Head of Internal Audit

Cumberland Building Society

Content

- Background to the FSA Business Continuity Guide
- Implications for Cumberland Building Society
- Examples of GAP analysis
- Actions resulting from Gap Analysis
- Role of Internal Audit

Background

- 2005 the FSA, Bank of England and HM Treasury carried out the “Resilience Benchmarking Project” with the aim to:
 - assess resilience and recovery capability of the UK financial services sector in the event of a **major operational disruption**

A major operational disruption is an incident:

- *that would have widespread impact on more than one organisation,*
- *that has a severe impact on firms*
- *requires the implementation of special arrangements for continued operation.*

Background (cont)

- Over 60 firms were questioned
- Answering over 1000 questions on their business continuity arrangements.
- From this, the Business Continuity Management Practice Guide was developed.
- Guide is available for all institutions to use - www.fsa.gov.uk/pubs/other/bcm_guide.pdf
- The Guide is based on real examples of standard and leading practice.

The Guide

- The Guide has been designed to:
 - help regulated firms with their business continuity planning.
 - stimulate thinking around business continuity planning and crisis management arrangements.
 - **it does not form part of the FSA's formal rules and guidance.**
- It should **not** be viewed as a definitive checklist of steps to take but rather as a flexible tool to stimulate thinking:
 - firms should be mindful of their individual circumstances (risk profiles) when considering what may or may not be appropriate.
 - firms are encouraged to take a pragmatic and sensible view of which aspects of the Guide are most useful and relevant.

The Guide (cont)

- Examples of observed practice are grouped by topic
 - Corporate Continuity
 - Corporate Crisis Management
 - Corporate Systems
 - Corporate Facilities
 - Corporate People
- The above capture the various components of business continuity planning and provide a framework for building resilience and recovery capability.

The Guide (cont)

- Two levels of observed practice are identified in the Guide:
 - Observed standard practice (adopted by most)
 - Observed leading practice (adopted by highest scoring 20% of the 60 benchmarking participants)

Impact on Cumberland Building Society

- Established a Business Continuity Committee (Headed by an Executive member) - key TOR are:
 - To consider adequacy of Business Continuity Plan
 - To update Business Continuity Plans as required
 - To review results of Business Continuity tests
 - To consider and agree the frequency and types of Business Continuity tests that are undertaken.
- Completed a gap analysis against the Guide - action plan agreed.

Business Continuity Guide (Corporate Continuity)

Std Ref	Observed Standard Practice	Comply (Yes/ No)	CBS Comment or Action required to comply	FILE REF
SECTION A	CORPORATE CONTINUITY			
A 1	Business Continuity Planning (BCP)			
A1.1.1	Risk Assessment			
A1.1.1	<i>Detailed risk assessments</i> are carried out annually or when there is a change in normal operations.	Yes		
A1.1.2	All impact assessments are current and have been reviewed and updated in the past year.	Yes		BCP Plan SR Management Report
A1.2	BCP Strategy			
A1.2.1	• A BCP reflecting identified risks exists for all departments.	Yes		BCP Plan
A1.2.2	• Plans consider time of the day, year and other business cycles.	Yes		BCP Plan
A1.2.3	• Plans have identified the impact to business in a disaster for all functions and they specify timescales and priorities for recovering these functions.	Yes		BCP Plan BCP Server Recovery Timescales
A1.2.4	• Plans reflect the impact a major operational disruption would have on the business.	Yes		BCP Plan
A1.2.5	• Planning considers total destructive loss of the site and any operational disruption including some loss of staff.	Yes		BCP Plan
PLUS Leading Practice	Planning considers <i>wide area destruction and anyoperational disruption involving significant loss of staff.</i>	Yes		BCP Plan
A1.2.6	• Plans are written and owned by decentralised plan owners. Alternatively, centralised plans are written by the Business Continuity function with departmental plans maintained by decentralised plan owners.	Yes		Monthly Procedure Manual Maintenance forms BCP 6-monthly sign-off
A1.2.7	• Web-based plans are accessible anywhere but all key staff also carry quick reference cards. Alternatively, a mix of paper, reference cards and/or electronic and/or web-based is accessible at all times.	Yes		C-Net BCP Plan at BCP site
A. 2	BCP Design			
A.2.1	Critical Suppliers			
A.2.1	Firm has liaised with critical suppliers regarding their arrangements.	Yes		BCP Plans, Server Recovery Timescales 3 rd party contracts
PLUS Leading Practice	Critical suppliers are involved in tests on an at least annual basis.	Yes		

Business Continuity Guide (Corporate Crisis Management)

Std Ref	Observed Standard Practice	Comply (Yes/ No)	CBS Comment or Action required to comply	FILE REF
SECTION B	CORPORATE CRISIS MANAGEMENT			
B.1	CULTURE			
B.1.1	Strategy			
B.1.1.1	A detailed current crisis management plan is in place.	Yes		BCP Plan
B.1.1.2	The crisis management plan contains instructions on how to respond to the issue of casualties and fatalities.	No		
B.1.1.2 Leading Practice	Instructions on responding on the issue of casualties and fatalities <i>have been verified during tests.</i>	No		
B.1.1.3	The crisis management strategy allows operations to continue indefinitely, allowing for some reduction of throughput.	Yes		Crisis Management Plan
B.1.1.3 Leading Practice	The crisis management strategy allows operations to continue indefinitely <i>with no reduction of throughput.</i>	Yes		Crisis Management Plan
B.1.2	Audit and Review			
B.1.2.1	Adjustments to the plan are made when threats change significantly.	Yes		Quarterly Procedure Manual Sign-off (held by Internal Audit)
B.1.2.1 Leading Practice	There is a regular formal review and update process, irrespective of changes of threats.	Yes		Quarterly Procedure Manual Sign-off (held by Internal Audit)
B.1.3	Accessibility			
B.1.3.1	The crisis management plan is accessible in a mix of media including: <ul style="list-style-type: none"> • paper plans; • electronic plans; • web-based plans; and • reference cards which are accessible at all times. 	Yes		BCP Plan C-Net
B.1.4	Senior Management			
B.1.4.1	The executive management team knows who is in the crisis management team and has approved their selection.	Yes		Crisis Management Plan
B.1.4.2	The executive management team understands the crisis management team's remit. They have agreed to them running the crisis, approved their empowerment and signed off the plan.	Yes		Crisis Management Plan
B.1.4.3	The agreed roles of the executive or senior management during an incident are contained in the crisis management plan and they have been signed off by the individuals concerned.	Yes		Crisis Management Plan
B.1.4.4	If the senior management team is located overseas, UK offices are aware of its plan to manage a crisis.	N/a		

Business Continuity Guide (Corporate Systems)

SECTION C	CORPORATE SYSTEMS			
C.1	IT			
C.1.1	Identification of Risks			
C.1.1.1	Plans identify: • points of consistency of data for recovery; • consequences of allowing non-affected systems to continue when others are non-operational; and • any unique critical system (and its recovery is reflected in the plans).	Yes		
C.1.2	Identification of critical IT			
C.1.2.1	A fully detailed impact analysis on loss of IT has been performed to identify which of the organisation's IT systems and infrastructure are the most business critical.•	Yes		6-monthly sign-offs
C.1.2.2	There is an ongoing continuous process or cycle to analyse and document the criticality of the organisation's IT systems	Yes		6-monthly sign-offs
C.1.2.3	A systematic dependency analysis has been performed covering most critical areas of IT to evaluate the impact of an individual IT system failure.	Yes		
C.1.2.3 Leading Practice	A <i>fully detailed and authorised IT dependency analysis</i> has been performed to evaluate the impact of an individual IT system failure.	No		
C.1.3	Recovery IT restoration plans address the following -			
C.1.3.1	Restoration of all IT systems according to business conditions	Yes		BCP Plans
C.1.3.1 Leading Practice	There are <i>detailed procedures for prioritising IT recovery</i> according to business conditions.	Yes		BCP Plans
C.1.3.2	the time needed to recover IT at all critical sites;	Yes		BCP Plans Server Recovery Timescales
C.1.3.3	all aspects of critical systems recovery is carried out by the firm's staff;	Yes		BCP Plan IT Disaster Plan
C.1.3.4 Leading Practice	There are plans to restore the development environment.	No but see comment		
C.1.3.5	restoration of connectivity to critical networks;	Yes		BCP Plans
C.1.3.6	restoration (including tests) of critical computer systems and associated hardware;	Yes		IT Disaster Plan
C.1.3.7	where mirror systems are used, backup devices and software are in place to manage backups from a single replicated system when the primary has failed	Yes		IT Ops Section 5
C.1.3.8	permanent connections to recovery sites to recover wide area network communications for systems and users;	Yes		IT Disaster Plan IT BCP Plan
C.1.3.9	eventual recovery of every system; and	Yes		BCP Plans

Business Continuity Guide (Corporate Facilities)

D.	CORPORATE FACILITIES			
D.1.1	Planning			
D.1.1.1	On-site non-company building managers are required to be involved in verifying site emergency plans.*	N/a		
D.1.1.2	If occupancy of buildings is mixed, tenants' plans are required to conform with the building manager's Continuity plan	N/a		
D.1.1.3	Plans include vacating recovery sites once recovery is complete.	No		
D.1.2	Energy			
D.1.2.1	All critical business functions are protected by uninterruptible power supply (UPS) or similar battery backup.	Yes		IT Ops Section 6
D.1.2.1 Leading Practice	<i>All areas and systems</i> are protected by uninterruptible power supply or similar battery backup	No		
D.1.2.2	All areas and systems have their power supply backed up by generators	Yes		
D.1.2.3	Power can be provided by generator(s) for at least three days using on-site stored fuel.	No		
D.1.2.3 Leading Practice	Power can be provided by generator(s) for <i>at least one week</i> using on-site stored fuel. •	No		
D.1.2.4	If the gas supply to the area is discontinued, functions at the site can still operate indefinitely because alternative sources of energy are in place	N/a		
D.1.3	Water			
D.1.3.1	If the water supply to the area is discontinued or becomes contaminated, the site can remain open at least two days.	Yes		
D.1.3.1 Leading Practice	If the water supply to the area is discontinued or becomes contaminated, the site can remain open <i>at least one week</i> .	Yes		
D.1.4	Security			
D.1.4.1	All critical sites have security guards (24 hours a day, 7 days a week), internal and external CCTVs, access control systems and a standard security procedure for receiving couriers and visitors.	No/Yes		
D.1.4.2	Physical access to critical areas and floors is restricted by guards' presence and individual swiped card or similar (e.g. biometrics).	No		
D.1.4.3	Permanent and temporary staff, contract staff and visitors required to wear visible id badges.	Yes		HO Admin Instructions

Business Continuity Guide (Corporate People)

E.	CORPORATE PEOPLE			
E.1.1	BCP Awareness			
E.1.1.1	Business continuity is included in induction programmes for new employees.			
E.1.1.2	Most staff are aware of the organisation's business continuity strategy and of the roles, responsibilities and organisation of the business continuity team.			
E.1.1.2 Leading Practice	<i>All staff</i> are aware of the organisation business continuity strategy and of the roles, responsibilities and organisation of the business continuity team.			
E.1.1.3	Senior management and most staff are familiar with their role during a major operational disruption.			
E.1.1.3 Leading Practice	<i>All staff</i> are familiar with their intended role during a major operational disruption.			
E.1.1.4	Plans clearly state which staff are required at the recovery site and which can go home and this has been tested.			
E.1.1.5	Staff know whether they might be sent home in an incident.			
E.1.1.6	All HR staff have been trained and have been involved in business continuity tests.			
E.1.1.7	HR strategy supports business continuity.			
E.1.1.8	More than 90% of managers know their planned staffing levels in an incident.			
E.1.2	Training			
E.1.2.1	Most staff at all grades and contractors have received business continuity training.			
E.1.2.2	Staff who might be called upon to deal with sensitive issues (such as working on a casualty helpline) have been trained.			

Impact on Cumberland Building Society (cont)

ACTION POINTS ARISING FROM THE GAP ANALYSIS (Highlighted in red above)

Std Ref	Observed Standard Practice	Comply (Yes/ No)	CBS Comment or Action required to comply	FILE REF
A.3.2.1 Leading Practice	More than 20% of UK staff have business continuity as part of their objectives.		1.	
A.3.3.1	<ul style="list-style-type: none"> Plans reflect consultation of local emergency services' response plans and include reference materials. 			
A.3.3.1 Leading Practice	<ul style="list-style-type: none"> Local authority emergency plans and emergency services' response plans are reflected in the plan. 			
A.3.3.2	<ul style="list-style-type: none"> Plans take into account provisions of the Civil Contingencies Act. 			
A.4.1.1 Leading Practice	There is a clear, documented and approved audit cycle covering all locations and functions.			
A.4.1.2	Business continuity planning appears on Board's agenda at least twice each year.			
A.4.1.3	Business continuity planning appears on Risk and Audit committees' agendas at least every quarter.			
A.4.3.3	Out-of-hours telephone contact tests are conducted at least once per year*			
A.4.3.6	The testing schedule is current and published within the organisation.			
B.1.1.2	The crisis management plan contains instructions on how to respond to the issue of casualties and fatalities.			
B.1.1.2 Leading Practice	Instructions on responding on the issue of casualties and fatalities <i>have been verified during tests.</i>			
B.2.4.1 Leading Practice	The crisis management team is provided with planned and pre-identified staff during a crisis to provide operational support (e.g. assistants, analysts and auditors).			
C.1.5.1	There is an up-to-date and detailed network diagram in IT plans.			
C.1.6.3 Leading Practice	If buildings and content and non-replicated data were destroyed, this would create no noticeable backlogs or impact on operations.			

Role Of Internal Audit

Undertake an annual audit to ensure that effective controls are in place (and are being used) to mitigate the Key risk:

“Failure to have adequate arrangements in place to ensure business continuity”

Key controls in place and therefore tested include:

Business continuity plan, Business Continuity Committee,

Business Continuity testing, Business continuity procedures,

6 monthly logisitcs sign off, 6 monthly procedural manual sign off,

Annual IT testing of branch connectivity and live internet banking,

BCP Site >1km from site and contains all required security, fire controls and back up of IT systems

Findings are reported to the BCP Committee and the Audit and Risk Committee.

Any Questions?