Financial Services Authority

Business Continuity Management Practice Guide

November 2006

Contents

Business Continuity Management Practice Guide

Introduction 1

How to use the Guide 2

How the FSA will use the Guide 4

Table of contents 5

A. Corporate Continuity 6

B. Corporate Crisis Management 13

C. Corporate Systems 18

D. Corporate Facilities 26

E. Corporate People 29

Business Continuity Management Practice Guide

Introduction

Background

During 2005, the Tripartite Authorities (FSA, Bank of England and HM Treasury) carried out the Resilience Benchmarking Project[1]. The project was designed to assess the resilience and recovery capability of the UK financial services sector in the event of major operational disruption such as a terrorist attack or natural disaster. We define major operational disruption as an incident having widespeard impact on more than one organisation, that has a severe impact on firms, and that requires the implementation of special arrangements for continued operations of critical business functions.

The project provided us with a valuable insight into the overall business continuity preparedness of more than 60 firms that took part in the Benchmarking exercise, answering more than 1,000 questions on their business continuity arrangements. With their agreement we have produced this Business Continuity Management Practice Guide in the spirit of sharing lessons learned from the project so that firms that did not participate can also benefit from it. The Guide is based on real examples of standard and leading practices we observed in the firms that participated. It reflects the collective business continuity planning and crisis management expertise of the UK's most significant firms and financial infrastructure providers.

Purpose

The Business Continuity Management Practice Guide is not general guidance from the Tripartite Authorities, nor is it guidance on FSA rules. Rather, it aims to help regulated firms in their business continuity planning by identifying and

1 For more information see www.fsc.gov.uk/upload/public/Files/9/Web%20-%20Res%20Bench%20Report%2020051214.pdf.

sharing examples of business continuity practice observed in firms that participated in the benchmarking exercise. We hope that these observations may be useful for firms when reviewing their own business continuity and crisis management arrangements. Firms should not view the Guide as a definitive checklist of steps to take, but rather as a flexible tool to stimulate their thinking and provide a framework for the development of their own plans. Above all else, firms should continue to be mindful of their individual circumstances and risk profiles when considering what may – or may not – be appropriate for their business.

Examples of observed practice are grouped by topic and organised by theme into modules:

Corporate Continuity

Corporate Crisis Management

Corporate Systems

Corporate Facilities

Corporate People

The modules capture the various components of business continuity planning and testing and provide a framework for building resilience and recovery capability. By defining clearly elements of processes like risk identification or crisis team activation, the Guide may help firms improve their business continuity planning.

How to use the Guide

Observed standard practice – observed leading practice

Two levels of observed practice are identified within the Guide:

- ***Observed standard practice*** generally reflects the practices adopted by most of the 60 benchmarking participants.

- ***Observed leading practice*** generally reflects the practices adopted by the highest scoring 20% of the 60 benchmarking participants, and tends to denote more robust or sophisticated practices.

In a handful of cases we exercised discretion and included examples of observed standard practice which did not meet the above criteria, but which we considered helpful or important to include nonetheless. These instances represent fewer than 7% of all of the examples of sound practice contained in this Guide.

Risk based approach

This Guide is not intended to be a comprehensive list of all the business continuity practices relevant to a financial firm. Therefore, the FSA does not expect firms to take a tick-box approach to using the Guide. Instead, firms are encouraged to take a pragmatic and sensible view of which aspects of the Guide are most useful and relevant for them. For example, firms may wish to:

- 'Mix and match' across observed standard and leading practices as they see fit, adapting their plans to reflect their individual risk profile and the complexity of their activities.

- Exercise common sense when deciding which aspects of the Guide are most relevant to them. For instance, various examples of observed leading practice may be more relevant to very large firms or firms with very large exposure to specific markets, whereas smaller or less complex firms may not necessarily need to have such sophisticated plans.

- Adopt more sophisticated arrangements than the examples provided as observed leading practice.

Differentiating between observed standard practice and observed leading practice

- Observed standard practice sets out the general practice observed in each area. The corresponding observed leading practice either supplements or completely replaces the observed standard practice. For an example of where observed leading practice replaces observed standard practice, refer to Module A Section 3.3.1.

- Where observed standard and leading practice appear to be very similar, the key differences are shown in italics. For an example of this, refer to Module A Section 3.3.3.

- In some cases we have set out observed standard practice only. This is because we have either not observed a higher standard, or because only a very small number of benchmarking participants met a higher standard. For an example of this, refer to Module A Section 3.2.2.

- In other cases, we have set out observed leading practice only. This is because there were insufficient responses to justify its inclusion as standard practice; however, we considered it

sufficiently important to merit inclusion as a positive example of good business continuity practice. Consequently, these examples have been included as observed leading practice, with no corresponding standard example. For an example of this, please refer to Module A Section 2.2.1.

How the FSA will use the Guide

The Guide does not form part of the FSA's formal rules and guidance. So, just as we would expect firms to exercise their common sense and judgement regarding which aspects of the Guide are likely to be most relevant to them, supervisors will be similarly pragmatic. We anticipate that the Guide will provide a useful basis around which firms and their supervisors can structure their discussions on business continuity planning, while bearing in mind that individual firms' arrangements should be proportionate to the nature and scale of their business and appropriate to their individual risk profile.

Table of contents

A. Corporate Continuity	B. Corporate Crisis Management	C. Corporate Systems	D. Corporate Facilities	E. Corporate People
A.1 Business continuity planning	***B.1 Culture***	***C.1 Information Technology (IT)***	***D.1 Planning***	***E.1 Staff***
A.1.1 Risk assessment	B.1.1 Strategy	C.1.1 Identification of risks	D.1.1 Planning	E.1.1 BCP awareness
A.1.2 BCP strategy	B.1.2 Audit and review	C.1.2 Identification of critical IT	D.1.2 Energy	E.1.2 Training
A.2 BCP design	B.1.3 Accessibility	C.1.3 Recovery	D.1.3 Water	E.1.3 Staff planning
A.2.1 Critical suppliers	B.1.4 Senior management	C.1.4 Providers	D.1.4 Security	E.1.4 Key staff
A.2.2 Responding to requests for BCP information from third party organisations	***B.2 Team***	C.1.5 Network resilience	D.1.5 Evacuation	E.1.5 Checks
A.2.3 Outsourcing contract providers	B.2.1 Crisis management team	C.1.6 IT resilience	D.1.6 Emergency services	E.1.6 Tests
A.2.4 Critical paper assets	B.2.2 Team activation	C.1.7 Data	D.1.7 Testing	***E.2 Crisis management***
A.3 Resources	B.2.3 Team attributes	C.1.8 Security		E.2.1 Contacting staff
A.3.1 BCP team	B.2.4 Team support	C.1.9 Site		E.2.2 Staff welfare
A.3.2 Staff and BCP	B.2.5 Facilities	C.1.10 Alternate site		
A.3.3 Third parties and BCP	***B.3 Communications***	C.1.11 Review, audit and changes		
A.4 Plan review	B.3.1 Communication strategy	C.1.12 Testing		
A.4.1 BCP audit	B.3.2 Internal and external communications	***C.2 Telephony***		
A.4.2 BCP changes		C.2.1 Recovery		
A.4.3 Testing		C.2.2 Site		
A.4.4 Documentation		C.2.3 Testing		
A.4.5 Recovery service providers				
A.5 Recovery times for critical functions				
A.5.1 Trade clearing				
A.5.2 Settlement				
A.5.3 Wholesale payments				

Business Continuity Management Practice Guide

A. Corporate Continuity

A.1 Business Continuity Planning (BCP)		Observed standard practice	Observed leading practice
A.1.1 *Risk assessment*	A.1.1.1 A.1.1.2	• *Detailed risk assessments* are carried out annually or when there is a change in normal operations. • All impact assessments are current and have been reviewed and updated in the past year.	
A.1.2 *BCP strategy*	A.1.2.1 A.1.2.2 A.1.2.3 A.1.2.4 A.1.2.5 A.1.2.6 A.1.2.7	• A BCP reflecting identified risks exists for all departments. • Plans consider time of the day, year and other business cycles. • Plans have identified the impact to business in a disaster for all functions and they specify timescales and priorities for recovering these functions. • Plans reflect the impact a major operational disruption would have on the business. • Planning considers total destructive loss of the site and any operational disruption including some loss of staff. • 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. • 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.	As for observed standard practice but: • Planning considers *wide area destruction and any operational disruption involving significant loss of staff*.

A.2 BCP design		Observed standard practice	Observed leading practice
A.2.1 Critical suppliers	A.2.1.1	• Firm has liaised with critical suppliers regarding their arrangements.	• Critical suppliers are involved in tests on an at least annual basis.
A.2.2 Responding to requests for BCP information from third party organisations	A.2.2.1		• Firm supplies evidence of its capability and testing.
A.2.3 Outsourcing contract providers	A.2.3.1	• Requirements on providers are included in formal terms in the contract.	• Requirements on providers, *including participation or auditing of tests*, are included in formal terms in the contract.
A.2.4 Critical paper assets	A.2.4.1 A.2.4.2 A.2.4.3 A.2.4.4 A.2.4.5	• Critical paper assets are managed through systematic classification according to criticality. • Critical paper assets are filed on a managed basis and put in fireproof cabinets to avoid destruction. • Replicated paper records can be accessed within one working day of an incident. • Scanned data for critical functions can be recovered and used at recovery site immediately.	As for observed standard practice but: • Critical paper assets are managed with a *classification scheme that includes impact or criticality*. • Critical paper documentation is replicated on a managed basis within one week of creation or change. • Scanned data can be recovered and used at recovery site immediately *for all data*.

A.3 Resources		Observed standard practice	Observed leading practice
A.3.1 *BCP team*	A.3.1.1 A.3.1.2	• Most team members are competent in all disciplines or areas defined by the Business Continuity Institute. • Team members understand critical functions and are able to represent most of their continuity interests.	As for observed standard practice but: • *All* team members are competent in all disciplines or areas defined by the Business Continuity Institute. • Team members *fully* understand critical functions and are able to *converse fluently* with *specialists in each critical area*.
A.3.2 *Staff and BCP*	A.3.2.1 A.3.2.2 A.3.2.3 A.3.2.4	• If there is a Trade Union presence in the organisation, it was consulted on BCP.	As for observed standard practice but: • More than 20% of UK staff have business continuity as part of their objectives. • If the plan's activation is expected to result in additional workload, the need and deployment of temporary or contract staff has been planned in detail. • Plans make provision for transportation of staff under certain disruption conditions.
A.3.3 *Third parties and BCP*	A.3.3.1 A.3.3.2 A.3.3.3	• Plans reflect consultation of local emergency services' response plans and include reference materials. • Plans take into account provisions of the Civil Contingencies Act. • Insurance policy details are included in the plans.	• Local authority emergency plans and emergency services' response plans are reflected in the plan. • Insurance details and procedures *agreed with insurers* are included in the plans.

A.4 Plan review		Observed standard practice	Observed leading practice
A.4.1 *BCP audit*	A.4.1.1 A.4.1.2 A.4.1.3	• Plans are subject to internal and external audit. • Business continuity planning appears on Board's agenda at least twice each year. • Business continuity planning appears on Risk and Audit committees' agendas at least every quarter.	As for observed standard practice but: • There is a clear, documented and approved audit cycle covering all locations and functions. • Business continuity planning appears on Board's agenda *at least every quarter.*
A.4.2 *BCP changes*	A.4.2.1 A.4.2.2	• Business continuity is always considered as part of a formal change control process ensuring all relevant components are reviewed before change takes place. • Business continuity documents are updated when a test is completed or when a major change occurs.	As for observed standard practice but: • Detailed risk and impact assessments and plan updates are carried out to build business continuity into a change in management processes.
A.4.3 Testing	A.4.3.1 A.4.3.2 A.4.3.3 A.4.3.4 A.4.3.5 A.4.3.6	• At least 75% of all business functions have been tested in the last two years. • Tests involve integrated simulation, involving IT, facility and critical staff recovery using alternate facilities. • Out-of-hours telephone contact tests are conducted at least once per year. • Representatives from all areas and at all levels, including senior management, are involved in tests. • Neighbouring businesses and emergency services are consulted about testing. • The testing schedule is current and published within the organisation.	As for observed standard practice but: • Out-of-hours telephone contact tests are conducted *at least once every six months*. • All staff are involved in tests. • Neighbouring businesses and emergency services are involved in some tests.

A.4.4 Documentation	A.4.4.1 A.4.4.2	• Pre-test documentation is available before testing. • After the test, reports are all completed with clear actions and owners.	
A.4.5 Recovery service providers	A.4.5.1		• If recovery service providers are used, their capacity to cope with multiple concurrent usage has been tested.

A.5 Recovery times for critical functions		Observed standard practice	Observed leading practice
A.5.1 Wholesale payments		The firm avoids entering into new business unless it is confident it can meet its obligations as they fall due.	From the point of invocation all material pending transactions falling due that day are settled by close of business. On the next working day the following transactions are settled by close of business: • Any outstanding transactions falling due the previous day that have been rolled over; • All transactions falling due that day.
A.5.2 Trade clearing		The firm avoids entering into new business unless it is confident it can meet its obligations as they fall due.	From the point of invocation all material pending transactions falling due that day are settled by close of business. On the next working day the following transactions are settled by close of business: • Any outstanding transactions falling due the previous day that have been rolled over; • All transactions falling due that day.
A.5.3 Settlement		The firm avoids entering into new business unless it is confident it can meet its obligations as they fall due.	From the point of invocation all material pending transactions falling due that day are settled by close of business. On the next working day the following transactions are settled by close of business: • Any outstanding transactions falling due the previous day that have been rolled over; • All transactions falling due that day.

Business Continuity Management Practice Guide

B. Corporate Crisis Management

B.1 Culture		Observed standard practice	Observed leading practice
B.1.1 *Strategy*	B.1.1.1 B.1.1.2 B.1.1.3	• A detailed current crisis management plan is in place. • The crisis management plan contains instructions on how to respond to the issue of casualties and fatalities. • The crisis management strategy allows operations to continue indefinitely, allowing for some reduction of throughput.	As for observed standard practice but: • Instructions on responding on the issue of casualties and fatalities *have been verified during tests.* • The crisis management strategy allows operations to continue indefinitely *with no reduction of throughput.*
B.1.2 *Audit and review*	B.1.2.1	• Adjustments to the plan are made when threats change significantly.	• There is a regular formal review and update process, irrespective of changes of threats.

B.1.3
Accessibility
	B.1.3.1	• The crisis management plan is accessible in a mix of media including:
		  • paper plans;
		  • electronic plans;
		  • web-based plans; and
		  • reference cards which are accessible at all times.	

B.1.4 *Senior management*	B.1.4.1 B.1.4.2 B.1.4.3 B.1.4.4	• The executive management team knows who is in the crisis management team and has approved their selection. • 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. • 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. • If the senior management team is located overseas, UK offices are aware of its plan to manage a crisis.	

B.2 Team		Observed standard practice	Observed leading practice
B.2.1 *Crisis management team*	B.2.1.1 B.2.1.2 B.2.1.3 B.2.1.4 B.2.1.5 B.2.1.6 B.2.1.7	• The crisis management team is responsible for managing all critical internal and external issues to resolution. • The crisis management team has a clear and formal structure. • Responsibilities and alternates exist for all roles. • At least 70% of crisis management team members and deputies have been involved in tests or incidents in the past 12 months. • The core crisis management team may be supplemented by pre-selected and trained specialists according to incident type, scale and severity. • The crisis management team has demonstrated capability in tests. • The crisis management team's membership is stable, and any necessary changes kept to a minimum.	

B.2.2
Team activation
	B.2.2.1
	B.2.2.2
	B.2.2.3
		• The crisis management team is invoked following certain agreed disruptive circumstances.
		• The crisis management team can be activated according to defined escalation mechanism.
		• Following activation, the team is formed by one or more of these options according to circumstances:
		  • conference call with further assembly at an agreed location (primary or secondary);
		  • pre-defined standard meeting places and times; and
		  • assembly at a pre-defined location or secondary location.	

B.2.3 *Team attributes*	B.2.3.1 B.2.3.2	• Once activated, the crisis management team has full authority for all decisions. • The crisis management team has clear spending powers during a crisis (their use and extent have been pre-approved).	
B.2.4 *Team support*	B.2.4.1	• The plan provides for named individuals to be seconded to the crisis management team to provide operational support on an as-needed basis.	• 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).
B.2.5 *Facilities*	B.2.5.1 B.2.5.2 B.2.5.3	• If the site is inaccessible, the crisis management team is accommodated in a pre-prepared primary or secondary location at least on kilometre from the affected site. • If the site can still be used, the crisis management team is accommodated in a pre-prepared crisis management room or command centre. • The primary command centre location to support the crisis management team is fully equipped to operate as a dedicated crisis command centre (e.g. stationery, telephones, printers, PCs, TVs, desks, conferencing).	

B.3 Communications		**Observed standard practice**	**Observed leading practice**
B.3.1 Communications strategy	B.3.1.1 B.3.1.2 B.3.1.3	• The crisis management communication plan covers internal and external communications with staff, peer organisations, the media and other stakeholders. • There is a clearly defined process for dealing with the media and public relations during a crisis and it has been verified during tests. • The crisis management team including key communications staff, and general management are familiar with the crisis management communications plan.	As for observed standard practice but: • *All staff* with specific requirements placed on them by the plan are familiar with the crisis management communications plan.

B.3.2 Internal and external communications	B.3.2.1
	B.3.2.2
	B.3.2.3
		• The external communications or public relations plan has been tested responding to crises affecting the organisation.
		• Telephone or mobile phone call cascade or automated calling systems are used for communicating instructions and status information to staff at the start of a crisis.
		• During a crisis staff can contact the business through:
		  • a telephone number that they know they can call; and/or
		  • a widely publicised 24-hour manned emergency contact number.
			• Dedicated web pages or recorded message or call centre contact are used for communicating instructions and status information to staff at the start of a crisis.

Business Continuity Management Practice Guide

C. Corporate Systems

C.1 IT		**Observed standard practice**	**Observed leading practice**

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).	

C.1.2 Identification of critical IT	C.1.2.1 C.1.2.2 C.1.2.3	• 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. • There is an ongoing continuous process or cycle to analyse and document the criticality of the organisation's IT systems. • A systematic dependency analysis has been performed covering most critical areas of IT to evaluate the impact of an individual IT system failure.	As for observed standard practice but: • A *fully detailed and authorised IT dependency analysis* has been performed to evaluate the impact of an individual IT system failure.

C.1.3 Recovery		IT restoration plans address the following:	As for observed standard practice but:
	C.1.3.1	• restoration of all IT systems according to business conditions;	• There are *detailed procedures for prioritising IT recovery* according to business conditions.
	C.1.3.2	• the time needed to recover IT at all critical sites;	
	C.1.3.3	• all aspects of critical systems recovery is carried out by the firm's staff;	
	C.1.3.4		• There are plans to restore the development environment.
	C.1.3.5	• restoration of connectivity to critical networks;	
	C.1.3.6	• restoration (including tests) of critical computer systems and associated hardware;	
	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;	
	C.1.3.8	• permanent connections to recovery sites to recover wide area network communications for systems and users;	
	C.1.3.9	• eventual recovery of every system; and	
	C.1.3.10	• the return of IT operations to their original site.	

C.1.4 Providers	C.1.4.1	• All critical sites use more than one telecoms provider for voice and data. The following interactions take place with providers:
		  • planned formal meetings take place to plan resilience of the communications network;
		  • planned verification takes place to check the resilience of telecoms providers' network architecture and of the connectivity and routing within it; and
		  • verification of IT third party suppliers' disaster recovery capability.
			As for observed standard practice but:
			• Continuous interaction with planned formal meetings takes place to plan resilience into communications network.
			• Detailed planned and formal reviews take place to verify the resilience of telecoms providers' network architecture and of the connectivity and routing within it.

	C.1.4.2	• Procedures as to how the disaster recovery providers will manage a multiple invocation of their sites is known, documented and agreed;	
	C.1.4.3	• Assurance has been given by providers that separacy/diversity services are in place in the wide area network.	

C.1.5 *Network resilience*	C.1.5.1 C.1.5.2 C.1.5.3 C.1.5.4 C.1.5.5 C.1.5.6	• There is an up-to-date and detailed network diagram in IT plans. • All aspects of network continuity are proactively and formally managed. • Networks are designed to be fully redundant with no single points of failure. • Network availability figures are monitored for trends as well as threshold exception basis and the information is used to identify points of weakness. • The full control and visibility of wide area network assets needed to provide end-to-end separation can be demonstrated (e.g. through documentation) internally. • Wide area network communications can be restored at work area recovery sites in less than one hour.	As for observed standard practice but: • The full control and visibility of your wide area network assets needed to provide end-to-end separation can be demonstrated (e.g. through documentation) internally *and externally*.
C.1.6 *IT resilience*	C.1.6.1 C.1.6.2 C.1.6.3 C.1.6.4 C.1.6.5	• No critical system depends on an individual person for restoration in a disaster. • Critical IT systems are spread across diverse locations. • If buildings and content and non-replicated data were destroyed, this would create backlogs smaller than one week. • In an incident affecting the most critical IT site, all of the affected critical IT systems could be recovered within four hours from invocation. • If replicated critical systems are used and both sites are lost, recovery can still take place.	As for observed standard practice but: • If buildings and content and non-replicated data were destroyed, this would create no noticeable backlogs or impact on operations. • In an incident affecting the most critical IT site, all of the affected critical IT systems could be recovered *within two hours from invocation*. • If replicated critical systems are used and both sites are lost, recovery can still take place *within agreed business timeframes*.
C.1.7 *Data*	C.1.7.1 C.1.7.2	• All critical data are copied or they are replicated at another site. • It takes less than one hour to retrieve off-site copies of critical recovery data (where applicable).	

C.1.8 *Security*		IT security elements include the following elements:	As for observed standard practice but:
	C.1.8.1	• Firewalls that are compliant with the organisation's current security policy and that have been compliance tested through regular penetration testing.	
	C.1.8.2	• Recognised standard of encryption for all critical communications is used internally and externally.	• Recognised standard of encryption for all critical communications is used internally and *externally and in storage*.
	C.1.8.3	• The usage of removable storage devices on desktops is restricted and anti-virus deployed.	• The usage of removable storage devices on desktops is *permitted only to authorised devices*.
	C.1.8.4	• Anti-virus products are deployed at external network entry points, on mail servers and on all desktops and laptops.	
	C.1.8.5	• Anti-virus products are automatically updated when released by vendor.	
	C.1.8.6	• Laptops are barred from connecting to the network unless they are authorised by IT security first.	
	C.1.8.7	• Vendor operating systems patches are reviewed for impact and relevance and tested before being applied.	
	C.1.8.8	• Escrow agreements are used to protect key software.	
	C.1.8.9	• Documented information security policy is current and formally refers to ISO17799.	
C.1.9 *Site*	C.1.9.1	• The IT environment has separate physical access control.	
	C.1.9.2	• The IT environment power supply to critical systems is protected with UPS and generators.	
	C.1.9.3	• IT environment humidity, ventilation and air-conditioning are controlled.	
	C.1.9.4	• IT environment is protected by fire detection and suppression.	
	C.1.9.5	• IT environment is protected by water detection.	

C.1.10 *Alternate site*	C.1.10.1 C.1.10.2 C.1.10.3 C.1.10.4 C.1.10.5 C.1.10.6	• There is an alternate dedicated site where IT is restored following a disaster located at least ten kilometres away from the main site. • There is an access to source code on core systems at the recovery site. • The bandwidth from work area to recovery site is adequate to handle needs in a disaster scenario (100% of the bandwidth can be redirected to the recovery site in 24 hours). • Detailed recovery plans exist for the redirection of all feeds from each primary site to respective recovery sites. • There is a mechanism for invoking the secondary site if the primary recovery site is not available.	As for observed standard practice but: • There exists a secondary recovery site that can be used if the primary recovery site is unavailable.
C.1.11 *Review, audit and changes*	C.1.11.1 C.1.11.2 C.1.11.3 C.1.11.4	• Continuity is always considered as part of a formal change control process ensuring all relevant components are reviewed before change takes place. • The criticality of IT systems is reviewed at least every six months. • Where outsourcing is used, critical IT outsourcing companies' business continuity management capabilities are audited. • All changes go through an agreed and signed-off procedure.	As for observed standard practice but: • The criticality of IT systems is reviewed on a *major change* or at least every six months – whichever is first.
C.1.12 *Testing*	C.1.12.1 C.1.12.2 C.1.12.3 C.1.12.4	• IT recovery tests are required to realistically reflect the worst case scenario where all critical systems must be restored concurrently. • Critical systems recovery is tested every six months. • Where a test environment is used, it is very similar to the live environment. • Where some IT functions are outsourced, critical IT outsource companies participate individually in tests.	As for observed standard practice but: • Where a test environment is used, it is *identical* to the live environment. • Multiple critical IT outsource companies participate concurrently in tests for incidents affecting sites.

	C.1.12.5	• If some IT aspects are outsourced, a policy to test outsourcers' IT disaster recovery capability exists.	

	C.1.12.6	• The following elements are tested:
		  • Identified critical application or hardware and/or software keys.
		  • Market data feeds and systems at the disaster recovery site (tested to the best of ability due to external constraints).
		  • Operation of market data and other critical third party feeds are tested at each disaster recovery site where they will be used, as applicable.
		  • Rebuilding of client or desktop environment.
		  • Remote home working recovery capability to the disaster recovery site, and adequate capability is evidenced.
		  • Restoration of critical applications: live tests from mirrored systems or backups on an un-configured system are run.
		  • If mirrored systems are used, the operation of each secondary system with the primary switched off is tested.
		  • If critical backups are needed, they are restore-tested every month.
		  • Unscheduled recall of offsite copies of critical recovery data.
			Tests have the following additional features:
			• *All* market data feeds and systems at the disaster recovery site.

	C.1.12.7	• Individual restoration tests suggest that all critical applications can be recovered in the required timeframes.	• *Concurrent restoration* tests suggest that all can be recovered in the required timeframes.

C.2 Telephony		Observed standard practice	Observed leading practice
C.2.1 *Recovery*		Recovery plans include:	As for observed standard practice but:
	C.2.1.1	• Company telecommunications resilience and recovery strategy to divert calls.	
	C.2.1.2	• ACD, IVR and turrets in call centre restoration, where applicable.	
	C.2.1.3	• Telephone conferencing system capabilities are planned to be restored.	
	C.2.1.4	• Redirection of non-geographic incoming phone lines (0800, 0870 etc), if they are used.	
	C.2.1.5	• Adequate fax facility at the recovery site.	
	C.2.1.6	• Voice communications recovery strategy can be implemented within two hours of invocation.	• The voice communications recovery strategy can be implemented in less than one hour from invocation.
	C.2.1.7	• 100% of voice lines can be redirected to an appropriate alternative location (e.g. recovery site, call centre) within 24 hours of invocation.	• More than 100% (in case of an increase in call volume) of voice lines can be redirected to the recovery site within 24 hour from invocation.
	C.2.1.8	• At least 80% of business as usual call throughput (including fax and modem) can be handled by the recovery site provisions.	• Normal call throughput (including fax and modem) can be handled by the recovery site provisions.
C.2.2 *Site*	C.2.2.1	• For all sites, where the option exists, there is a policy for two or more physical entry points or ducts for voice communications fibres and/or cables.	
	C.2.2.2	• There are connections to multiple external telephone exchanges at each critical site.	
C.2.3 *Testing*	C.2.3.1	• Telephony recovery test takes place at least annually at each critical site. As part of this, the following elements are tested:	• Telephony recovery is tested *every six months* at each critical site.
	C.2.3.2	• mobile phone reception at recovery site;	
	C.2.3.3	• redirection of telephony to the recovery site;	• Voice communications can be redirected to the recovery site and have been tested in the past six months.
	C.2.3.4	• the programming of the telephone PABX used in recovery; and	
	C.2.3.5	• the restoration of critical telephony.	

Business Continuity Management Practice Guide

D. Corporate Facilities

D.1 Planning		Observed standard practice	Observed leading practice
D.1.1 *Planning*	D.1.1.1 D.1.1.2 D.1.1.3	• On-site non-company building managers are required to be involved in verifying site emergency plans. • If occupancy of buildings is mixed, tenants' plans are required to conform with the building manager's continuity plan. • Plans include vacating recovery sites once recovery is complete.	
D.1.2 *Energy*	D.1.2.1 D.1.2.2 D.1.2.3 D.1.2.4	• All critical business functions are protected by uninterruptible power supply (UPS) or similar battery backup. • All areas and systems have their power supply backed up by generators. • Power can be provided by generator(s) for at least three days using on-site stored fuel. • 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.	As for observed standard practice but: • *All areas and systems* are protected by uninterruptible power supply or similar battery backup. • Power can be provided by generator(s) for *at least one week* using on-site stored fuel.
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.	• If the water supply to the area is discontinued or becomes contaminated, the site can remain open *at least one week*.
D.1.4 *Security*	D.1.4.1 D.1.4.2 D.1.4.3	• 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. • Physical access to critical areas and floors is restricted by guards' presence and individual swiped card or similar (e.g. biometrics). • Permanent and temporary staff, contract staff and visitors required to wear visible id badges.	As for observed standard practice but:

	D.1.4.4	• Sites use 'battle boxes'. Alternatively, firms keep and maintain the materials they need to help them to recover their operations off-site, and in a secure location.	
	D.1.4.5	• Where battle boxes are used site occupants are able to retrieve battle boxes from the point of demand within two hours.	• Site occupants are able to retrieve battle boxes from the point of demand within one hour.
	D.1.4.6	• A clear desk policy is in operation.	
	D.1.4.7	• A policy for controlling introduction of packages or items means that there is a dedicated post room which systematically scans for threatening objects.	
	D.1.4.8	• Advanced fire detection and early warning systems are installed.	
	D.1.4.9	• The air-conditioning system has auto-shut-off if there is a fire, smoke detection or CBRN alert.	
	D.1.4.10	• There are water detection systems in all vulnerable or high flood-risk areas.	
	D.1.4.11	• The site is protected against electrical spikes and surges (e.g. lightning strikes).	
D.1.5 Evacuation	D.1.5.1	• A designated trained senior manager or their deputy always takes responsibility for managing evacuation.	
	D.1.5.2	• Invacuation points have been identified and clearly marked for all staff.	
	D.1.5.3	• There is a clear demonstrable way of ensuring the building is clear (e.g. electronic records, roll call).	
	D.1.5.4	• A secondary evacuation point is located at least 500m away from primary evacuation points.	
D.1.6 Emergency Services	D.1.6.1	• Emergency services are aware of all critical site emergency plans.	
D.1.7 Testing			As for observed standard practice but:
	D.1.7.1	• Full fire evacuation tests are required at each critical site annually.	
	D.1.7.2	• Both generators and UPS are full-load tested on an at least bi-annual basis.	• Both generators and UPS are full-load tested on an *at least quarterly basis.*

Business Continuity Management Practice Guide

E. Corporate People

E.1 Staff		Observed standard practice	Observed leading practice
E.1.1 *BCP awareness*	E.1.1.1 E.1.1.2 E.1.1.3 E.1.1.4 E.1.1.5 E.1.1.6 E.1.1.7 E.1.1.8	• Business continuity is included in induction programmes for new employees. • Most staff are aware of the organisation's business continuity strategy and of the roles, responsibilities and organisation of the business continuity team. • Senior management and most staff are familiar with their role during a major operational disruption. • Plans clearly state which staff are required at the recovery site and which can go home and this has been tested. • Staff know whether they might be sent home in an incident. • All HR staff have been trained and have been involved in business continuity tests. • HR strategy supports business continuity. • More than 90% of managers know their planned staffing levels in an incident.	As for observed standard practice but: • *All staff* are aware of the organisation business continuity strategy and of the roles, responsibilities and organisation of the business continuity team. • *All staff* are familiar with their intended role during a major operational disruption.
E.1.2 *Training*	E.1.2.1 E.1.2.2 E.1.2.3	• Most staff at all grades and contractors have received business continuity training. • Staff who might be called upon to deal with sensitive issues (such as working on a casualty helpline) have been trained. • All executives, managers and designated critical staff have trained deputies who can fulfil their duties.	As for observed standard practice but: • All executives, managers and designated critical staff *have first and second-level trained deputies* who can fulfil their duties.

E.1.3 *Staff planning*	E.1.3.1 E.1.3.2	• All staff contracts make provision for working from alternative or recovery sites. • Working Time Directive requirements are considered in BCP.	
E.1.4 *Key staff*	E.1.4.1 E.1.4.2 E.1.4.3	• There is a policy preventing key staff from travelling together. • Risk mitigation means that the loss of critical staff in a disaster would have a limited impact on operations.	As for observed standard practice but: • Uniquely skilled individuals are identified and cross-training or other formal measures are provided to reduce the risk. • Risk mitigation means that the loss of critical staff in a disaster would have a *negligible* impact on operations.
E.1.5 *Checks*	E.1.5.1 E.1.5.2 E.1.5.3	• At least two references are always requested and checked for new employees. New employees are also background security checked. • References are always requested and checked for contractors, including agency temps. • Contractors who will perform sensitive functions are security checked.	As for observed standard practice but • The checks are repeated periodically. • *At least two references* are always requested and checked for contractors, including agency temps. • Contractors who will perform sensitive functions are security checked *and the checks are repeated*.
E.1.6 *Testing*	E.1.6.1	• Specialist HR support providers are involved in continuity-related tests and exercises.	

E.2 Crisis Management		Observed standard practice	Observed leading practice
E.2.1 Contacting staff	E.2.1.1	• There is a detailed procedure to ensure that all staff staying at home during any recovery are kept informed.	

E.2.2 Staff welfare	E.2.2.1	• To provide for the assurance of staff welfare, plans have one or more of the following:
		  • procedures are in place for designated staff and managers to ensure staff welfare needs are met;
		  • contracts are in place to identify and provide all affected staff with liaison, support and counselling following a disruption; and
		  • there are procedures in place to enlist specialist care and welfare services and direct them to affected staff.	

	E.2.2.2	• Plans include provision for managing staff fatalities.	
	E.2.2.3	• Plans consider a level of staff fatalities.	
	E.2.2.4	• Next-of-kin information for staff is available on evacuation.	

The Financial Services Authority
25 The North Colonnade Canary Wharf London E14 5HS
Telephone: +44 (0)20 7066 1000 Fax: +44 (0)20 7066 1099
Website: http://www.fsa.gov.uk