BCM Risk Matrix

The matrix below identifies key aspects of BCM which authorities believe firms should consider in their business continuity strategies and planning (Column 1). The main risks arising from these issues are set out in Column 2. Columns 3 and 4 are currently empty. Our intention is to populate these columns with standard and best practice in BCM. We aim to do this in two ways. Firstly, by publishing the matrix on the website we are giving firms the opportunity to contribute to the identification of standard and best practice by sharing their own experiences of BCM with us. We would encourage firms wishing to participate in this exercise to download a copy of the matrix (in Word format), complete columns 4 and 5, and submit to FSA (email businesscontinuity@fsa.gov.uk). Secondly, FSA is conducting a number of detailed BCM reviews with a selection of firms. This information will also inform our work on identifying current standard and best practice. Once the matrix has been populated we will publish further information on this website.

Figure 1 BCM Risk Matrix

1	2	3	4
Issue	**Risk Factors**	**Observed Standard Practice**	**Observed Best Practice**
BCM Organisation			
Is a member of the senior management team responsible for BCM?	▪ Failure to secure senior level responsibility and support for BCM can reduce the ability of the firm's BC manager to engage the business areas. This creates a risk that the BCP will not accurately capture the risk profile of the business. The plan may therefore prove inadequate in a disaster situation.	▪	▪
How does the firm ensure that Disaster Recovery team members understand their objectives and the reporting structure?	▪ Poor awareness creates a risk that BCM staff will be unable to carry out their duties effectively in the event of a disaster. This exposes the firm to significant operational and reputational risk.	▪	▪
Is each business unit head or nominee aware of the disaster recovery reporting structure and plan?	▪ Business unit involvement in BCM is essential. Failure to involve business unit heads creates a risk that local BCM responsibilities will not be taken seriously enough and staff may be unable to discharge them effectively. This lowers the probability of a successful BCP implementation in the event of a disaster.	▪	▪
Clear escalation route for BCM decisions to Senior Management?	▪ Where escalation procedure is not clearly specified, there is a risk that quality and timeliness of BCM decisions may be adversely affected. Ineffective decision-making may result in sub-optimal resource utilisation and lead to weaknesses in the BCP, thereby increasing the firm's risk profile.	▪	▪
Is there a dedicated BCM budget?	▪ Where spending on BCM is cyclical, discretionary rather than dedicated, and not directly linked to the organisation's risk profile, there is a risk that BCM will be insufficiently funded and planning may therefore be sub-optimal.	▪	▪

1	2	3	4
Issue	**Risk Factors**	**Observed Standard Practice**	**Observed Best Practice**
Business Impact Analysis			
Has the firm identified plausible threats from both internal and external sources and assessed impact and probability?	▪ Failure to identify and assess the impact/probability of plausible threats creates a risk that the firm's BCP will not match the firm risk profile and may therefore be limited in its effectiveness during a disaster.	▪	▪
Has the firm introduced controls to mitigate against the effects of identified threats?	▪ Upgrading the BCP is only part of the response to threat assessment. The firm should also consider using this data to introduce controls/safeguards to reduce the likely effect of these threats. Failure to do this increases the likelihood that the full impact of these events will be felt should they materialise.	▪	▪
Has the firms identified its critical business units?	▪ Failure to identify and prioritise critical business units means that the BCP will be sub-optimal. Vital time may be lost in trying to recover non-critical areas. This increases the firm's risk profile and jeopardises the success of the recovery.	▪	▪
Were the main business units involved in preparing the BIA?	▪ The BCM team should involve the critical business units in identifying plausible threats. Otherwise there is a risk that the BIA does not capture all plausible risks to the business.	▪	▪

1	2	3	4
Issue	**Risk Factors**	**Observed Standard Practice**	**Observed Best Practice**
Interdependency Mapping			
Has the criticality of business functions and records been defined, and priorities established?	▪ Failure to identify and prioritise critical business functions and processes means that the BCP will be sub-optimal. Vital time may therefore be lost in recovering non-critical areas. This increases the firm's risk profile.		
Have interdependencies between critical business functions and systems been determined?	▪ The interdependency of key business functions and systems should be fully mapped and regularly reviewed. This recognises that a crisis in one area can have an immediate knock-on effect in other areas. Failure to map interdependencies means that the BCP will not fully capture the firm's risk profile. This creates a risk that the firm's ability to respond to a disaster will be diminished.		
Have critical business projects been catered for in interdependency mapping?	▪ Recovery of critical business and IT projects should be included in the BCP. Interdependencies between projects, and between projects and business units, should be identified and contingencies established where appropriate. Whilst failure to do this may not affect initial recovery of critical operations, it may pose a serious risk to long-term success of the business.		
Business Continuity Plan			
Does the BCP reflect the needs of key parts of the business?	▪ Critical business units should be consulted when drawing up/revising the BCP. Without this, there is a risk that the BCP does not adequately prepare the business for the risks reflected in the BIA.	▪	▪
Has the firm set clear priorities for functions that must be maintained whilst operating under the BCP?	▪ Setting clear priorities for recovering key business functions/processes focus the BCP on high risk areas and prevents the firm from wasting valuable time during a disaster. Failure to establish priorities will undermine the firm's capacity to execute its BCP.	▪	▪
Has the BCM team explained to the	▪ Key assumptions should be identified and clarified with the business in preparing the BCP. It is vital	▪	▪

1	2	3	4
Issue	**Risk Factors**	**Observed Standard Practice**	**Observed Best Practice**
business the key assumptions on which the BCP is based?	that the business fully understands and is accountable for any assumptions made. Without this there is a risk that the BCP does not fully reflect current business realities and this may reduce the effectiveness of business recovery.		
Is the BCP (and key assumptions) regularly tested and revised?	▪ The firm should implement a regular BCP testing programme. Failure to test means that opportunities to improve the plan are missed. In real crisis situations the BCP may prove to be deficient.	▪	▪
Information and Telecommunications Systems			
Have all critical IT systems been identified and prioritised and their recovery time periods defined?	▪ IT systems and data security is critical to the survival of the firm. Failure to identify and prioritise critical systems means that the BCP will be sub-optimal. Vital time may therefore be lost in recovering non-critical systems. This increases the firm's risk profile.	▪	▪
Arrangements in place for the acquisition of critical IT resources at short notice?	▪ Prior arrangements which secure delivery of IT/IS hardware in the event of disaster save time and reduce the risk hardware shortages.	▪	▪
Have critical bespoke applications/ spreadsheets/databases been identified and included in IT backup plans?	▪ Mapping of critical business systems tends to focus on highly visible systems. However, a number of firms depend on bespoke, stand-alone applications to carry out key processes on which more "orthodox" systems rely for key data. Failure to include these in the BCP can impair the efficiency of the firm's recovery.	▪	▪
Were end-users involved in identifying bespoke applications? What procedures are in place for identifying new applications?	▪ End-users should be involved in identifying bespoke applications and a procedure should be established to notify the BCM team when new applications have been developed. Otherwise there is a risk that a critical application will not be included in the BCP.	▪	▪

Outsourcing – Disaster Recovery Provision			
Is there a documented SLA between the firm and its DR provider?	▪ There should be a documented service level agreement in place which makes explicit the expected performance levels of the supplier. The service provider should supply regular management information against these performance metrics. ▪ Absence of a SLA makes it difficult to measure performance levels and the accountability of the supplier is therefore more ambiguous.	▪	▪
Has the firm undertaken a cost/benefit analysis of the choice between dedicated and syndicated space?	▪ Undertaking a cost/benefit analysis allows the firm to make an informed decision and to allocate its BCM budget efficiently.	▪	▪
If the firm is using a mix of dedicated and syndicated recovery space, what evidence exists of a risk-based allocation to different business units?	▪ The firm should take a risk-based approach to allocating dedicated versus syndicated recovery space between business units. The most high risk areas should be allocated dedicated space. ▪ Failure to allocate space on this basis means that the BCP will be sub-optimal given the firms risk profile. Key people may be deprived of recovery space where there are competing claims to syndicated space.	▪	▪
Is the firm advised when its syndicated site is occupied (invocation notice)?	▪ It is important that the SLA commits the service provider to notifying the firm when the disaster recovery site has been invoked by another firm. The firm should have a backup plan to cover the period of invocation (normally up to 13 weeks). Failure to do so raises the firm' s risk profile considerably during this period.	▪	▪
Does the firm know: the total number of additional claims per syndicated seat; details of the	▪ Before contracting with a provider, the firm should be fully aware of the risks of using syndicated space (e.g. competing claims). The firm should check the provider's backup plans to cope with multiple invocations. Without this information the firm execution of its BCP may be seriously	▪	▪

providers' backup plans and arrangements for providing alternative space?	compromised.		
Where the firm is renting dedicated space, has it tested its plans? E.g. to move staff to the recovery site, test the efficiency of IS and IT systems at the site, etc.	▪ Failure to test the service provider's ability to cope with invocation of the firm's BCP means that opportunities to improve both the firm's plans, and the provider's own arrangements, are missed. In a real disaster situation implementation of the firm's BCP may be at risk due to the provider's inadequate arrangements.	▪	▪
Outsourcing of core business processes or functions			
Does the firm have a BCP/disaster recovery plan in place that provides for continuation of the service from an alternative site?	▪ The firm should ensure that the BCP considers all material outsourced functions/processes. Failure to do this leaves the firm at risk of serious operational, reputational, or financial difficulties.	▪	▪
Is the plan regularly tested?	▪ The firm should implement a regular BCP testing programme. Failure to test suppliers' BCPs means that opportunities to improve the plans are missed. In real crisis situations the plans may prove to be deficient.	▪ The firm requires copies of all supplier BCP test results. These are reviewed by the operational risk managers in the appropriate business areas. ▪ Staff at the firm are aware of their responsibilities but no testing of this undertaken as yet.	▪ Supplier undertakes regular contingency exercises that test its ability to recover from disaster and maintain business continuity. The firm participates in these tests and reviews test results.
Does SLA specify the service provider's priorities for recovery?	▪ The firm should know how the service provider will react in a crisis and reflect this in its own BCP. A key piece of information is the relative priority the provider attaches to its various customers. This will influence the timing of service recovery, a key input into the BCP.	▪	▪
Has the firm prepared a standby plan to cover the event of a rapid	▪ However, the firm should also have a documented plan in place to cover the event of a rapid withdrawal from the contract. The absence of a standby plan may delay the bank's reaction time	▪ Outsourcing contracts normally include an exit plan as standard practice. This deals with situations in which an *orderly* withdrawal from the contract is	▪ None identified.

withdrawal from each contract?	should a rapid rather than an orderly withdrawal from a contract be required. There is therefore a greater risk that the bank's interests will not be protected should an unanticipated incident arise.	appropriate. ▪ No documented standby plan to cover the event of a *unanticipated exit* from a contract.	
Alternative BCM Strategies			
Have alternative recovery strategies been identified?	▪ The firm should regularly review its chosen BCM strategy bearing in mind the changing risks both within its business and the external environment. Failure to consider alternative strategies, such as altering the ratio of dedicated to syndicated recovery seats to reflect changing circumstances, creates a risk that the current BCP is not fit for purpose.	▪	▪
Have the risks associated with each optional recovery strategy been assessed against the business impact analysis?	▪ Alternative strategies should be assessed against the risks and priorities identified during preparation of the Business Impact Analysis. Failure to do this may result in sub-optimal strategies being implemented and this may reduce the effectiveness of the firm's BCP.	▪	▪
Has a cost/benefit analysis of alternative recovery strategies been prepared and presented to senior management?	▪ Assessments of alternative recovery strategies should include a cost/benefit analysis. Failure to do this creates a risk that a sub-optimal strategy will be implemented thereby increasing the firms risk profile.	▪	▪