

Business Continuity and Data Security in Financial Services



Business Continuity and Data Security planning are an essential part of good business practice. Both should be regarded as integral parts of a firm’s corporate governance and championed by senior management, a point which the Financial Services Authority (“FSA”) continues to reiterate. In an era of heightened due diligence, investors are also increasingly attuned to the value of these basic protections.

MMS Regulatory Solutions (“MMS RSL”) has devised a set of best practice procedures and benchmarking exercises that can help to ensure that you have suitably rigorous controls in place. This digest provides a summary of the key issues and demonstrates how we can help you with intelligent regulatory solutions.

Business Continuity

→ Introduction

The FSA insists that firms ensure they have a Business Continuity Plan in place at a strategic level.

The FSA’s rules on business continuity are contained within SYSC 4.1.6R – SYSC 4.1.8G. The rules state that a firm must take reasonable steps to ensure continuity and regularity in the performance of its regulated activities. To this end, a firm must employ appropriate and proportionate systems, resources, and procedures.

→ Business continuity policy (“BCP”)

A firm must establish, implement, and maintain an adequate business continuity policy aimed at ensuring, in the case of an interruption to its systems and procedures, that:

- > Any losses are limited
- > Essential data and functions are preserved
- > Regulated activities are maintained, or where this is not possible
- > Data and functions are recovered and regular activities are resumed in a timely manner

→ Key Recommendations

The matters dealt within a business continuity policy should include:

- > Resource requirements such as people, systems and other assets, and arrangements for obtaining these resources
- > The recovery priorities for the firm’s operations
- > Communication arrangements for internal and external concerned parties (including the FSA, clients, and the press)
- > Escalation and invocation plans that outline the processes for implementing the business continuity plans, together with relevant contact information
- > Processes to validate the integrity of information affected by the disruption
- > Regular testing of the business continuity policy in an appropriate and proportionate manner in accordance with FSA rules and best practice standards

Continued...



“Any testing undertaken by a firm should be documented, noting the event and highlighting the results of the test and any action taken to resolve any issues.”

Business Continuity continued...

→ Testing

Any testing undertaken by a firm should be documented, noting the event and highlighting the results of the test and any action taken to resolve any issues.

MMS Regulatory Solutions recommends that testing is completed on at least an annual basis.

→ Business continuity management and practice guide

Firms may wish to seek a copy of the FSA's Business Continuity Management Practice Guide http://www.fsa.gov.uk/pubs/other/bcm_guide.pdf. The guide is not deemed to be formal guidance on the FSA rules but rather aims to help firms in their business continuity planning by identifying and sharing examples of good practice observed in the industry.

Further, the Financial Sector Continuity website, designed to provide a central point of information about work on continuity planning is also a valuable resource. It can be found at:

www.financialsectorcontinuity.gov.uk

→ Benchmarking

Alternatively, you can let us take the strain. MMS Regulatory Solutions has developed a BCP benchmarking process designed to help you outline, monitor, and manage your continuity planning. Our review will help you deliver a comprehensive strategy, ensuring your business has the necessary and appropriate controls in place.

Data Security

→ Introduction

Financial services firms have always had an important duty to safeguard the personal data of their customers and clients. The FSA is increasingly focusing on whether firms are honoring that trust by having effective systems and controls to prevent data being lost or stolen. Personal data is being bought and sold by criminals who use it to steal identities and commit other crime. It is thus important that firms frequently review their controls and remain alert to new and ongoing threats.

→ FSA enforcement


The regulator has been taking an increasingly tough stance with the perpetrators of lax security. Merchant Securities Group Limited was fined £77,000 for poor data security practices. The company failed to adequately protect its customers from the risk of identity fraud.

The FSA has also fined Norwich Union £1.26m, BNP Private Bank £350,000 and Nationwide £980,000, for security lapses which compromised customers' personal data and placed individuals at risk of identity theft.

→ FSA thematic review

Previously, The Financial Crime and Intelligence Division ("FCID") conducted a thematic review of data-security controls, visiting 39 firms. It found that poor data security is a serious, widespread problem across the entire industry.

Continued...



“The FSA is increasingly focusing on whether firms are honoring that trust by having effective systems and controls to prevent data being lost or stolen.”

Data Security continued...

The shortcomings fall under three broad categories:

- > Failure to understand the risk
- > Lack of expertise to make an assessment of risk factors and devise ways of mitigating them
- > Failure to devote adequate resources to the issue

The review contends that firms need to stop underestimating the risk of harm that data loss and weak data management pose to their businesses. The FSA made it clear that it expects firms to be aware of its wider activities to combat the risks of financial crime.

“Getting data protection wrong can bring commercial, reputational, regulatory and legal penalties. Getting it right brings rewards in terms of customer trust and confidence”

Richard Thomas, Information commissioner

→ Key Recommendations

The FSA review details numerous examples of both best and bad practice. The good examples are extrapolated to form key recommendations targeted at smaller firms, and can be broadly outlined as follows:

- > Senior management should take responsibility for data security
- > Risk assessments are acted on as part of the monitoring process
- > Written policies and procedures

- > Detailed plans for reacting to data loss and communicating with customers as required
- > Simple guidance for all staff
- > Ongoing Monitoring to ensure that staff are not vulnerable to the temptation of data theft
- > Individual user accounts for client databases
- > Robust passwords containing a mixture of letters, numbers, and keyboard symbols
- > Secure disposal of confidential waste, using shredders or disposal services
- > Due diligence checks on third-party suppliers

→ Benchmarking

MMS RSL has developed a benchmarking exercise intended to encapsulate the recommendations above and provide a framework upon which sound data security risk management procedures can be based.

It will help focus your attention and ensure consideration is given to the risks posed by data security and requisite measures are in place to combat them.

MMS RSL will be happy to assist you with this exercise. We anticipate that it will lead to an enhancement in your controls and the mitigation of non business risks. In short, it is an exercise of real value.

It's our business to protect your business

We strive to provide all of our clients with the service they require in a flexible but structured way. At MMS Regulatory Solutions – one of the UK's leading compliance consultancies – we want you to relax knowing that your business is protected. If you wish to know more, please do not hesitate to get in touch.

Call us on **020 7065 5200**, email **info@mms-rsl.com** or visit our website at **www.mms-rsl.com**