Disaster Recovery testing and documentation

The FCA expects you to conduct a full disaster recovery test at least once per year. In practice this means that one business day needs to be devoted to a dry run of both a systems failure and lack of physical access to the normal office. Staff are instructed to work remotely from home or critical staff attend the disaster recovery site if the firm has one.

The purpose of this test is to demonstrate the successful fail over from the primary data centre and warehouse to the secondary, located at either another office or a dedicated disaster recovery site. It is also designed to show that firms have business continuity plans in place so that should a natural disaster or terrorist attack render both primary systems and offices inaccessible, business will continue with minimal disruption and no data loss.

The annual test and any issues flagged by the test for remedial action should be documented for presentation to the FCA on demand.

Systems fit for purpose

Your systems must be fit for purpose. This includes sufficient and secure document retention, trading systems that do not perpetuate flaws in the trading process or allow manual overrides of compliance controls and the capability to generate accurate and appropriate investor reporting.

Encryption

Data protection, both from a client and from a staff personal information perspective are very important. Any material data leak issues could result in investigations both from the FCA and the Information Commissioner's Office ('ICO'). Consequently, appropriate use of encryption is an expected way of preventing this. Excel and Word files containing sensitive information should be password protected and saved on a restricted access part of any shared drive.

Information sent outside the company should be encrypted to prevent emails sent by mistake from disclosing sensitive data.

Finally, some encryption may be essential to protect proprietary information such as preventing the unauthorised alteration of algorithms used for investment and trading purposes.

Portable devices and the risk of data loss

The loss of a smart phone, blackberry or laptop does happen and is a realistic part of business life. Such portable devices should be securely password protected and capable of being remotely wiped if identified as not recoverable.

Security: internal and external

IT must have suitable software in place to prevent network intrusions but also think about issues than may be caused internally. Common

practice is for personal email to be restricted, disc drives and USB port to be disabled and only used with prior permission.

We can assist with the preparation of disaster recovery plans and annual testing results that would meet FCA expectations, and can offer guidance on improvements to your current arrangements, therefore please contact us if you wish to discuss any of these aspects further.

Please contact us at:
Regent's Compliance
info@regentscompliance.com
0203 710 0142
07795261311
www.regentscompliance.com