

Outsourcing to cloud using



By

Adviser Cloud - Due Diligence Pack - November 2015

YOUR RESPONSIBILITY & THIS PAPER

The high-level regulatory obligations on outsourcing require a firm to appropriately identify and manage the operational risks associated with its use of third party outsource providers, including undertaking due diligence prior to making a decision on outsourcing.

This paper aims to identify areas in which Adviser Cloud believe we must support you in the continual, regular and habitual review of operational risk brought about by outsourcing.

PRIMARY RISKS AND OUR PROMISE

The FCA have identified the following primary risks associated with outsourcing to the cloud:

- The commoditised nature of many cloud services means cloud customers have less scope to tailor the service provided;
- The movement of customer data (in some cases, the customer can specify the geographic region in which their data must remain); and
- Firms using outsource providers who may contract out part of the service to other cloud providers, without customers initially being aware of the contracting out.

Our promise:

- We will continue to tailor our services for UK Wealth IFAs and Mortgage Brokers.
- We will only ever keep your data in the UK.
- We will always follow FCA guidance on outsourcing parts of our contracts and always make you aware of the firms we have outsourced to.

OUR EXIT GUARANTEE

We hope that you will remain happy with the services we provide to you but if you do decide to leave us we guarantee the following:

- We will only keep copies of your data that is required for the compliant and proper delivery of our services.
- Within one month of your contract finishing we will give you a copy of:
 - Your customer and client data on an unrestricted sql database or equivalent csv files.
 - Copies of your documents and files that have been stored on our cloud drives.
- We will never unreasonably deny you our full support to transition your data from our services to that of another provider.



AIM OF THIS DOCUMENT

The remainder of this document highlights key points and documents which we think collectively form due diligence on adviser cloud. Please double click where indicated to download and read the full documents to which the pictures refer. Where any link has broken, please let us know and will send you the relevant documents.

RELEVANT BACKGROUND:

We regard the following as important papers on this topic:

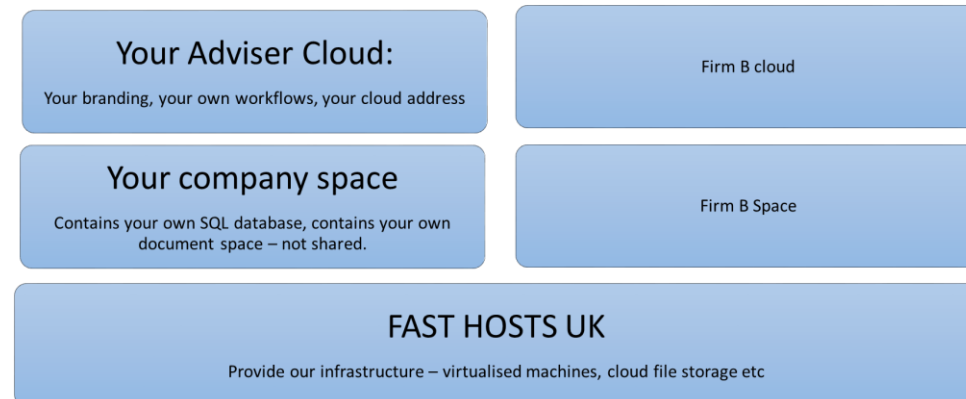
<https://www.fca.org.uk/static/documents/guidance-consultations/gc15-06.pdf>

http://www.fsa.gov.uk/pubs/other/data_security.pdf

<https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en>

<https://journal.uptimeinstitute.com/explaining-uptime-institutes-tier-classification-system/>

YOUR INFRASTRUCTURE



OUTSOURCING PLATFORM AND INFRASTRUCTURE

We have outsourced the platform infrastructure to UK Fast Hosts who also run our firewall services. Some key points:

- UK Fast Hosts are ISO 27001 accredited so you can be sure their data security standards reach acceptable levels for your business.
- UK Fast Hosts operate only Manchester Based Server Farms and if this changes we will let you know.
- UK Fast Hosts has a series of leading data and security accreditations
<https://www.ukfast.co.uk/accreditations.html>



- UK Fast Hosts is an UTI Level 3 accreditation.

UK FAST COMPLIANCE CERTIFICATE

CERTIFICATE OF REGISTRATION



This is to certify that the Management System of:

UKFast.Net Limited

UK Fast Campus, Birley Fields, Manchester, M15 5QJ

has been approved by ISOQAR



8396

ISO 27001: 2013

Scope of Activities:

All UKFast operations based out of Manchester Head Office with dedicated managed hosting provided from a number of datacentres in the UK. Statement of Applicability version 1.0 dated 12th August 2013 applies.

Certificate Number:	8396-ISO - 001
Initial Registration Date:	23 June 2010
Re-issue Date:	28 May 2015
Expiry Date:	23 June 2016

Signed by:
Steve Stubley, Technical Director
(on behalf of ISOQAR)

A handwritten signature in blue ink, appearing to read "Steve Stubley".

This certificate will remain current subject to the company maintaining its system to the required standard. This will be monitored regularly by ISOQAR. Further clarification regarding the scope of this certificate and the applicability of the relevant standards' requirements may be obtained by consulting ISOQAR. This certificate is one of several issued to registration number 8396.

ISOQAR Limited, Alcumus Certification, Cobra Court, 1 Blackmore Road, Stretford, Manchester, M32 0QY.
T: 0161 865 3699 F: 0161 865 3685 E: isoqarenquiries@alcumusgroup.com www.alcumusgroup.com/isoqar
This certificate is the property of ISOQAR and must be returned on request.



UK FAST ATTESTATION FOR COMPLIANCE – PCI DATA SECURITY



Payment Card Industry (PCI) Data Security Standard

Attestation of Compliance for Onsite Assessments – Service Providers

Version 3.1

April 2015

Section 1: Assessment Information

Instructions for Submission

PCI DSS Attestation of Compliance for Onsite Assessments – Service Providers, v3.1
© 2006-2015 PCI Security Standards Council, LLC. All Rights Reserved.

April 2015
Page 1

(Double click image to download)





SECURITY STATEMENT

This document is for UKFast clients only to provide more detailed information on the security policies and procedures. Client's actual security will vary depending on the type of solution that has been purchased. Solution specific details e.g. dedicated firewalls, operating system versions, anti-virus should all be handled separately.

Access Control Administration

PCI DSS and ISO 27001 have a number of requirements.

Please refer to the standards for more information.

- UKFast regularly audits access and deletes access rights in a timely and tractable manner.
- UKFast has specific accounts for accessing client solutions.
- Access to the administration of the UKFast network is highly restricted to the network team and the UKFast IT Director only.
- Our passwords follow PCI DSS standards which dictate password length, construction, rotation and threshold limits. These apply to both engineers and clients.
- UKFast only refresh passwords for clients with the PCI service.

Anti-virus Protection

UKFast does offer anti-virus protection to clients.

Please refer to specific solution for details and entitlement.

Application/User Layer

- Application security and authentication is not the responsibility of UKFast.
- Development and test environments are not the responsibility of UKFast unless taken as part of the solution.
- Live production data and its use is not the responsibility of UKFast.

Backups

- Accurate and complete records are kept of backups.
- Backup data is not encrypted.
- Backup data is not periodically validated.

Disclaimer Whilst UKFast has made every effort to ensure the accuracy of all the information and statements herein the accuracy, reliability, or completeness of the furnished data is not guaranteed or warranted in any way and UKFast and its representatives disclaim liability of any kind whatsoever, including, without limitation, liability for quality, performance, merchantability and fitness for a particular purpose arising out of the use, or inability to use the data.

06/11/2014 – UKFast client distribution only

(Double click image to download)



OUR DATA SECURITY ASSURANCE AND AUDITING POLICY

We strive to continually audit how we store and utilize your data and offer you the following assurance:

- Our data servers will always be hosted in the UK by appropriately accredited providers.
- Those providers must annually prove they have audited their policies to abide by current regulatory requirements.
- We will always backwards review and amend our policies to ensure we are aligned to the Financial Conduct Authority's current guidance on areas of IT and Data Security.
- We will conduct a six monthly internal review of our security policies and the effect they may have on your operations.
- When appropriate we will consult with external consultants to audit our software services including and not limited to an annual penetration test. We will forward you a copy of the results of these tests on request.
- We will always highlight any data breaches to you as soon as physically possible.
- We will review our data protection, password, information security and emergency escalation policies six monthly.
- We will ensure that our staff are trained on data prevention techniques and the consequences of data loss.

STANDARD RECOVERY - SYSTEM AUDITING

Company Settings - Users - Admin Tools - Automated Tasks - Module Configuration - Plugins -

Settings - Audit Log




Start Date: [] End Date: [] Email: support [v] AppW Filter [] Reset []

Log ID	Date Time	Action	Action Details	Username	First Name
59121	19/11/2015 15:10:43	Loaded ProductBaseControl Module	Audit Log	support@advisortcloud.co.uk	
59120	19/11/2015 15:10:43	The system auto configured the 'Audit Log' module.		support@advisortcloud.co.uk	
59119	19/11/2015 15:10:43	The system auto configured the 'Audit Log' module.		support@advisortcloud.co.uk	
59118	19/11/2015 15:10:43	The system auto configured the 'Audit Log' module.		support@advisortcloud.co.uk	
59117	19/11/2015 15:10:43	The system auto configured the 'Audit Log' module.		support@advisortcloud.co.uk	
59116	19/11/2015 15:10:43	The system auto configured the 'Audit Log' module.		support@advisortcloud.co.uk	
59115	19/11/2015 15:10:43	The system auto configured the 'Audit Log' module.		support@advisortcloud.co.uk	
59114	19/11/2015 15:10:43	The system auto configured the 'Audit Log' module.		support@advisortcloud.co.uk	
59113	19/11/2015 15:10:43	The system auto configured the 'Audit Log' module.		support@advisortcloud.co.uk	
59112	19/11/2015 15:10:43	Loaded ProductBaseControl Module	Audit Log	support@advisortcloud.co.uk	
59111	19/11/2015 15:10:43	The system auto configured the 'Audit Log' module.		support@advisortcloud.co.uk	
59110	19/11/2015 15:10:43	The system auto configured the 'Audit Log' module.		support@advisortcloud.co.uk	
59109	19/11/2015 15:10:43	The system auto configured the 'Audit Log' module.		support@advisortcloud.co.uk	
59108	19/11/2015 15:10:43	The system auto configured the 'Audit Log' module.		support@advisortcloud.co.uk	
59107	19/11/2015 15:10:40	The system auto configured the 'Audit Log' module.		support@advisortcloud.co.uk	
59106	19/11/2015 15:10:40	ViewSection	Settings Settings/Default.aspx	support@advisortcloud.co.uk	
59105	19/11/2015 15:10:35	Loaded ProductBaseControl Module		support@advisortcloud.co.uk	
59104	19/11/2015 15:10:35	Loaded ProductBaseControl Module		support@advisortcloud.co.uk	
59103	19/11/2015 15:10:35	ViewSection	Settings Settings/default.aspx	support@advisortcloud.co.uk	
59102	19/11/2015 15:10:28	Loaded ProductBaseControl Module		support@advisortcloud.co.uk	
59101	19/11/2015 15:10:27	Loaded ProductBaseControl Module		support@advisortcloud.co.uk	
59100	19/11/2015 15:10:27	ViewSection	Tasks Tasks/default.aspx	support@advisortcloud.co.uk	
59099	19/11/2015 15:10:27	The system auto configured the 'New Product Charges' module.		support@advisortcloud.co.uk	

We will provide your company administrators with the ability to see a fully audited log of all data changes on your database. This log enables us to recover data to former states if required.



STANDARD RECOVER – RECYCLE BIN

  Company Settings -  Users -  Admin Tools -  Automated Tasks -  Module Configuration -  Plugins -

ID	Type	Type ID	Details	Date Deleted	User Deleted	
1	Person	4	Paul Hogg	23/09/2015 16:23:54	support	Restore

Only adviser cloud employees can delete records from you system. If accidentally data is deleted it is stored in the recycle bin and you can restore this data when you require by simply clicking restore.

OUR ALWAYS AVAILABLE PROMISE

As part of our service guarantee we will provide the directors of your company with the mobile telephone numbers of the directors of Adviser Cloud to use in the case of any emergency.

DATA LOSS PREVENTION AND STAFFING

We control access to the infrastructure and only mandate access to our employees when they are sufficiently trained. We train each of our employees on the legal and client consequences of data loss and the need for each employee to be vigilant in the use of the data.

We do not allow employees to take data off our premises.

EXTERNAL DATA LINKS

We have tripartite agreements between you and the data provider firm. Each agreement is subject to its own terms and conditions and is governed between each of the parties under those agreements. Where Adviser Cloud receives data from a third party such as a wrap provider it is not responsible for the accuracy of that data.

We will only add data links to firms that have an industry accepted encryption policy.

ACCESS TO BUSINESS PREMISES AND RIGHT TO AUDIT

We will provide you with access to our business premises and offer you the right to audit our software and services at your own expense.

We would ask for at least one month's written notice of this audit.

Subject to our agreement we will allow this audit to be undertaken by your own auditors.



We will co-operate with the Financial Conduct Authority in any audit that they request during their regulation of your activity.

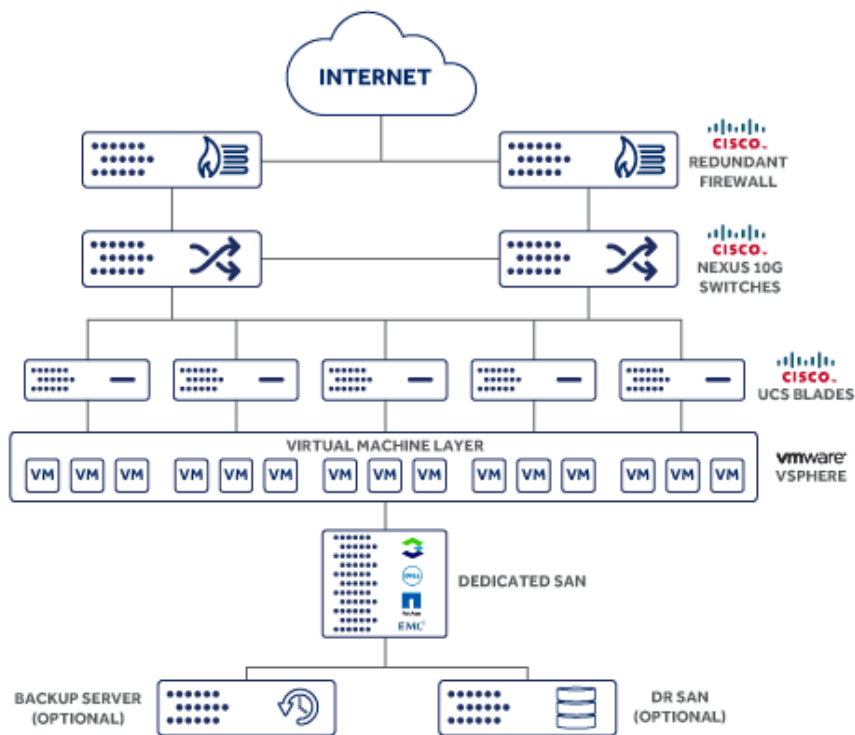
CHANGE MANAGEMENT

We follow agile change management processes. We use extended user acceptance testing where necessary to ensure effective delivery of new functionality.

We are happy for any one of our firms to become beta testers of our service and we promise to tell you of any significant developments and their release schedules so that you can plan any operational changes that may be appropriate.

DISASTER RECOVERY AND BUSINESS CONTINUITY

We operate on a private cloud provided by UK Fast Hosts and as such they offer us a 100% uptime guarantee – outside of scheduled maintenance which you will be made aware of.



Our redundancy policies allow us to enjoy the following SLA's for recovery in the event of disaster:

- 15 Mins with UK Fast
- 2 Hour Part Replacement.



PASSWORD SECURITY POLICY



Appendix 2 - Password Management Policy

1. POLICY PURPOSE:

This policy establishes conditions for use of, and requirements for appropriate security for Adviser Cloud accounts and passwords. These requirements are necessary to protect Adviser Cloud IT systems and data and to ensure that all users are aware of their responsibilities in effective password management.

1.1 Application

This policy applies to all users of Adviser Cloud and where applicable forms part of the user Terms & Conditions and Agreement.

1.2 Statement

Adviser Cloud shall develop, implement, and regularly review a formal, documented process for appropriately creating, modifying and safeguarding passwords used to validate a user's identity and establish access to the Adviser Cloud portal.

2. PASSWORD MANAGEMENT

2.1 General

Passwords are an important aspect of Adviser Clouds security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of network resources. As such, users (including contractors and vendors with access to Adviser Clouds system) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2.2 Process Requirements.

Adviser Clouds password management processes will include the following requirements:

- System-level passwords (e.g., root, enable, application administration accounts, etc.) will be changed every 90 days.
- System level passwords on stand alone or unshared systems may not need to be changed with the same frequency. For example, local user accounts who have administrative privileges on their workstations.
- User-level passwords for important systems/user roles (e.g. IT staff, key finance users) will be changed every 90 days.
- User accounts may not have system-level privileges with the exception of those users that have administrative privileges on their own workstations.
- Users that can justify system level access must request a separate admin account giving them specific system-level permissions for their applicable areas.

2.3 Password Rules.

- Create a strong password; see 2.5 General Password Requirements.
- It is the individual's responsibility to safeguard the password. Do not share Adviser Cloud passwords with anyone. All passwords are to be treated as sensitive, confidential; Adviser



Adviser Cloud Password Management Policy Jun 2013

(Double click image to download)



INFORMATION SECURITY POLICY



Adviser Cloud: Information Security Policy

1. Introduction

Adviser Cloud is a web based back office system designed for Independent Financial Advisers (IFA's). Adviser Cloud recognizes the need for its staff employed in management, technical support and administration to have access to the system and information they require in order to carry out their work and recognises the role of information security in enabling this. Security of information must therefore be an integral part of Adviser Cloud's management structure in order to maintain continuity of its business, legal compliance and to adhere to its own regulations and policies.

2. Purpose

This information security policy defines the framework within which information security will be managed across Adviser Cloud and demonstrates management direction and support for information security throughout Adviser Cloud.

3. Scope

This policy is applicable to, and will be communicated to, all Adviser Cloud employees that have access to the system be they employed by, or contracted to Adviser Cloud. It covers, but is not limited to:

- (i) any data attached to the Adviser Cloud system
- (ii) any information on telephone networks
- (iii) any communications sent to or from Adviser Cloud
- (iv) any data - which is owned either by Adviser Cloud, its partners or its clients
- (v) any data held on computers or other systems external to the Adviser Cloud system

4. Organisation of Information Security

The Managing Director is ultimately responsible for the maintenance of this policy and for compliance within Adviser Cloud. This policy has been approved by him and forms part of Adviser Cloud's policies and procedures.



Advisor Cloud Information Security Policy v1.0 Jun 2013

(Double click image to download)



DATA PROTECTION POLICY



Adviser Cloud
Data Protection Policy
November 2013

1. Introduction

This document sets out the obligations of Adviser Cloud ("the Company") with regard to data protection and the rights of people with whom it works in respect of their personal data under the Data Protection Act 1998 ("the Act").

This Policy shall set out procedures which are to be followed when dealing with personal data. The procedures set out herein must be followed by the Company, its employees, contractors, agents, consultants, partners or other parties working on behalf of the Company.

The Company views the correct and lawful handling of personal data as key to its success and dealings with third parties. The Company shall ensure that it handles all personal data correctly and lawfully.

2. The Data Protection Principles

This Policy aims to ensure compliance with the Act. The Act sets out eight principles with which any party handling personal data must comply. All personal data:

- 2.1 Must be processed fairly and lawfully (and shall not be processed unless certain conditions are met);
- 2.2 Must be obtained only for specified and lawful purposes and shall not be processed in any manner which is incompatible with those purposes;
- 2.3 Must be adequate, relevant and not excessive with respect to the purposes for which it is processed;
- 2.4 Must be accurate and, where appropriate, kept up-to-date;
- 2.5 Must be kept for no longer than is necessary in light of the purpose(s) for which it is processed;
- 2.6 Must be processed in accordance with the rights of data subjects under the Act;
- 2.7 Must be protected against unauthorised or unlawful processing, accidental loss, destruction or damage through appropriate technical and organisational measures; and
- 2.8 Must not be transferred to a country or territory outside of the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.



(Double click image to download)



EMERGENCY ESCALATION POLICY



Adviser Cloud: Emergency and Escalation Procedure

1. Introduction

Adviser Cloud is a web based back office system designed for Independent Financial Advisers (IFA's). Adviser Cloud recognizes the need for an emergency and escalation procedure in the event of a breach of its security, security policy or other disaster. The Managing Director, or person appointed by him, responsible for security, should maintain an awareness of threat and risk to the system and regularly review our processes.

2. Purpose

The purpose of this procedure is to provide a structure to the investigation, risk/damage assessment and restoration following, any system attack or breach, or any other violation of Adviser Cloud's security policy. The aim is to maintain system integrity, minimize disruption to clients whilst maintaining the highest level of security.

3. Scope

This policy is applicable to, and will be communicated to, all Adviser Cloud employees that have responsibility for the security of the Adviser Cloud system and its data.

4. Emergency and Escalation procedure.

- (i) A log must be maintained of all security events.
- (ii) The Managing Director, or person appointed by him, will complete and record a risk assessment of each event. The event will be categorised in the following way:
 - (a) LOW RISK – no additional action required.
 - (b) MEDIUM RISK – further investigation required.
 - (c) HIGH RISK - The system may have been compromised and should be taken off line whilst investigated.



Adviser Cloud Emergency and Escalation Procedure v1.0 Jun 2013

(Double click image to download)



FREQUENTLY ASKED QUESTIONS

PLATFORM SECURITY

When was the latest application and infrastructure vulnerability assessment and/or penetration test performed on your SaaS platform?

We test our firewall rules, port scan our external interfaces and ensure relevant application security is working via a series of URL tests to said application on a bi-daily basis.

Vulnerability testing for the infrastructure is provided under the ISO27001 standards implemented by UK Fast Hosts.

Where necessary we will also consult with external specialists annually to check for application vulnerability.

Are these performed as part of significant program changes, and part of your Software Development Lifecycle?

We try to operate a very dynamic Software Development Life Cycle, which results in a beta environment with restricted use, and a live version. Beta will only be applied to Live once it has undergone our extensive unit tests, which can be supplied in xlsx format upon request.

DEVELOPMENT & SECURE CODING

Who oversees and is responsible for your platform's development services?

Ian Jowett

David Wood

Racheal Smith

Where are the developers based?

Adviser Cloud's Head Office

How do they access the system?

Source code is accessed via Team Foundation Server, using VPN and Kerberos access. Web portals are accessed via a combination of FORMS, IP and custom authentication checks in Adviser Cloud code.

Please describe your secure coding methodology and controls.

Code is developed in small chunks, each small chunk is tested from the UI straight through to the underlying in house built libraries, this allows us to intercept calls from UI



to database/IO and test all inputs are secure, while ensuring back end data layers are free from injection, in the form of buffer-overflow, and via the use of Entity based frameworks and custom interfaces.

All user controls are built, tested and modified in house.

Can you elaborate more please on what methods or tools you use to check for application security vulnerabilities as the code moves from development/beta to production/live; such as database injection, buffer overflow attacks etc.

We use our own in built tools, aswell as visual studio and the Technical Director has over 10 years development experience which .net technologies and personally checks every line of code checked in.

Is real client data used in your development or test environments, if so, how are these additional secured similar to production?

Real data is never permanently used in development / test environments, however sometimes adviser cloud dev team may import an external file for the purpose of testing, and are either deleted or obfuscated afterwards.

Please describe your change management cycle.

We try to follow an AGILE methodology however in terms of precise detail:

- 1.1 Request comes from customer
- 1.2 Requests are grouped and prioritised
- 1.3 Work items are generated for each request in decided order.
- 1.4 Work items are developed and tested.
- 1.5 Successfully completed work items are tested internally and applied to beta.
- 1.6 Once beta has passed a full unit test, a site migration begins:
- 1.7 Site migration involves setting up second web site, applying xml changes to each customer database and migrating them to new tested live version.
- 1.8 Beta site begins second wave of development after all beta testers are migrated to latest release.
- 1.9 Second website is removed, and all customers are on live, latest, unit tested, secure version.

DATA CENTRE SECURITY

Where are your data centres based?

UKFast – Manchester Data Centre

To what UTI tiering level are these rated?

UKFast - Has a Level 3 Accreditation

If this is a fully or partial managed service, please provide details.

Service is partially managed and Advisercloud look after servers and software, UKFast look after infrastructure and firewall. Also Security and Intrusion detection is managed by UKFast.



What disclosure would you provide your clients if you relocated your data centers outside of the UK, even if on a temporary basis?

We will let you know via email of our intention to do this and will honor your need to ensure that it is stored on a minimum EU Safe Harbor standard.

STAFF SECURITY

Please describe your staff and contractor screening policy.

We don't use contractors, however all access to systems is screened by directors.

How do you educate staff & contractors of their security responsibilities?

We provide annual DPA, DLP and FCA compliance training similar to the competent persons requirements.

DATA BREACHES/SOC/CSIRT

What triggers would result in you notifying clients of a suspected or known data security breach?

If the system is breached we would get notified by email dependent upon the breach type, if a portal has been breached it will be audit logged and customer is told asap.

Do you have an in house or managed service to monitor for data security attacks and breaches?

Managed CISCO Redundant Pair, managed by UK Fast.

Please describe your controls in place to detect, block and alert against cyber security attacks.

UK Fast monitor cyber attacks, and is a service we receive from them, we also have everything audit logged in case of breach.

DATA SEGREGATION

What logical or physical separation exists to protect each client's data from others?

Each adviser cloud database exists on a secure Microsoft SQL Server, each database has its own database login with a unique, 16 digit alphanumeric password, with lots of symbols, this is then secured in a master database, using 3DES encryption, a salt and a 32bit private key.

What other controls are in place to ensure there is no mix of each of your client's data?

Our underlying data access library can only be initialized with client identifying information, i.e. FSA number, this means that in order for adviser cloud code to access their data pragmatically it would need specifically initialising using the secure username, password and details of the client.



Please describe your Data Loss Prevention approach and compensating controls.

All Web farm is clustered and based on a SAN everything is dual redundant.

Our staff will not be allowed to take data of site and we do not operate a bring your own device policy. All devices are owned and controlled by Adviser Cloud and encrypted as appropriate.

BCM/DR

Please describe your platform's backup and recovery architecture.

We use com Vault supplied to us from UK Fast, this takes snapshot of our web farm twice a day. We also use Hyper V Clustering, so a node failure will automatically transfer.

What encryption is in place to protect data in transmission to disaster recovery facilities (ie tape backups and/or data replication)?

There is no encryption as standard in place during the data transmission but does go over our secure network.

Our new data centre facility includes our Dedicated Backup Network™. This means that backup servers are run on a completely separate network to your main servers, with separate switches and connections, adding an extra level of redundancy to your backup solution but also a secure network that is not accessible to the outside world – therefore it is not encrypted as standard.

I have attached a high level PDF on the Commvault backup procedure and you can also find further information here:

http://documentation.commvault.com/commvault/v10/article?p=features/data_encryption/data_encryption.htm

How often are BCP & DR plans tested?

6 Monthly

Please describe the latest test scenario and results.

No issues, other results on request

What is your SLA on platform availability and recovery should an event occur?

15 Mins with UK Fast, 2 Hour Part Replacement.

