



Bluefin

Technical Information

Orbit Benefits Technology

Describe the hardware/software environment required for the Orbit Application.

Orbit is an internet application that is provided to the client as an internet service. All that is required is a compatible browser and internet access. No hardware or software is installed at the client site. An IT feasibility questionnaire should be completed which will enable us to determine that your client browser and network infrastructure is compatible.

Do you have a dedicated team that is responsible for IT Risk Management (e.g. IT Security, Disaster Continuity, Privacy)? If yes, please provide a description of the organisational model.

Yes. All aspects of risk management policy and procedures are the responsibility of the Executive Board of Bluefin Corporate Consulting. The Executive Board meets weekly and there are regular reports from the heads of Compliance and IT, who take individual responsibility for Privacy and Data Protection matters, IT Security, Business Continuity and overall risk management issues.

Orbit Technology Services are responsible for Orbit Benefits platform security and disaster recovery processes. This includes managing the outsourced IT security services to Vistorm.

Describe your company's database backup and archiving procedures, including schedule of backups, storage, encryption, details of third parties used.

Bluefin Data Backup and Disaster Recovery

We operate a comprehensive MPLS wide area network with Active Directory running across all our sites. Our detailed business continuity plans operate at both a national and local level. The plans in place cover IT and the delivery of core IT services to the business.

Our IT infrastructure is built on the basis that should any office be lost, the key information is still available from other locations or remotely owing to the replication process. Replication is undertaken by on-line backup, which snapshots information on a regular basis (four times each day) and stores it in a remote location accessible on our network. Tapes are also used to provide an additional layer of resilience.

We have a warm site disaster recovery centre which houses additional IT infrastructure, and also provides hot desks at four hours' notice. Because of the structure of our offices and locations, we are also able to provide connectivity from any of our other locations across the country.

In addition to this, we provide a remote access facility to key staff with access to data available from home, subject to appropriate security approval. This is provided through a number of firewalls and a hardware security appliance.

Each of our systems has been analysed whilst in use to determine the priority and how quickly they need to be operational in the event of an incident. Our key systems have built-in resilience which provides for an automatic failover. Other non-core systems will be operational within agreed timescales according to a service level agreement.

In addition there are local business continuity plans in place for each office, covering communication with staff. Each location has a crisis committee which assesses the extent of the situation and then determines what actions need to be taken in accordance with the various scenarios set out in the plans. The focus is mainly on staff, determining where they will be operating from and making sure this is communicated effectively.

The overall plan was last tested in September 2008, following a major upgrade to our core network operating systems. Although there were no significant findings from the test, it did lead us to update our plan to specify in more detail the allocation for hot desks and also increase the number of hot desks by 50%, with increased rack space to support our growing IT infrastructure.

Orbit Backup Procedures

Data backup is provided via the Cable & Wireless Data Centre service. This service includes maintenance and support of the backup software and there are agreed service levels for the commencement of backups and the fulfilment of restore requests.

The Cable & Wireless Shared Backup and Restore provides:

- Incremental on-line backup of daily changes.
- Full weekly on-line backup.
- Restore within 15 minutes of notification.
- Six-month retention of full backups.

Daily copies of the backup go to a separate on-disk backup server and this server is in turn backed up to tape. All servers have redundant disks and PSUs and each server has its own disaster recovery server. The tape backups are handled by a service hosted at the Cable & Wireless facility where the servers are located. In addition Orbit has built-in resilience of its database via Sun Clustering technology.

Do you utilise any third party vendor services for hosting or physical site services? If so, please provide the name of the vendor(s) and further details on the processes.

Orbit's servers are housed within a dedicated virtual data centre at a secure location operated by Cable & Wireless.

The service provides the following:

- The Virtual Data Centre Cage provides a secure area with steel mesh walls and a sliding access door that can be locked by a key.
- All power, air conditioning, smoke detection, fire suppression and security systems are monitored 24/7. Skilled staff are on duty at the data centre 24/7 to ensure all systems are operating correctly and to respond to any alerts. They also provide on-site support of the equipment by performing remote or hands-on maintenance and support tasks.

- Each data centre is connected to the Cable & Wireless global IP backbone, a single high-capacity IP network delivering integrated communications and consistent quality of service worldwide.

The following facilities are provided:

Power

The electrical power circuits at the Cable & Wireless Park Royal data centre are supplied via a redundant power system providing a capacity of 22.5 MVA. This system is supported by redundant:

- UPS of 28 x 400 kVA and 4 x 500 kVA (N+1 redundancy).
- Diesel generators providing 6 x 2.5 MVA and 6 x 1.5 MVA (N+1 redundancy) and equipped with 200,000 litres of fuel (enough for 72 hours of continuous operation when supporting a full load).

There is also a redundant power supply for each cage.

Environment

Each area within the Park Royal data centre is supported by a fully redundant air conditioning system (N+1 redundancy) and smoke detection systems are fitted throughout.

Fire suppression

The fire suppression systems within the Cable & Wireless data centre use a Hi-Fog Nitrogen system. Hi-fog combines the extinguishing characteristics of water with the penetrative qualities of gas, but without any safety hazards for personnel or the environment. Penetration and suppression of all types of fires is achieved by high-speed discharge of small water droplets in the form of a mist. Once activated, the Hi-fog system protects the space with high-density mist that easily reaches shielded areas, absorbs and blocks heat radiation from the fire source, and prevents oxygen from entering the combustion area. Due to the small amount of water employed, the system does not damage electrical or other equipment but at the same time maintains a safe environment for both equipment and personnel.

Security

Video camera surveillance systems incorporating over 300 cameras enable each floor area and external entrance to be monitored, 24/7. Physical access into the data centre and to the different areas inside the centre is controlled using an access card system and biometric readers. Security personnel are on site, around the clock, to control access to the data centre and monitor the security systems.

Does your organisation have practices in place to ensure compliance with all relevant privacy / data protection legislation?

Bluefin Corporate Consulting Limited is registered under the Data Protection Act as a Data Processor. Orbit has a published Data Protection Policy and Procedures handbook that is issued to all staff. There is also an Orbit Privacy Policy which informs customers of what Orbit can do with their data and how it is processed. The Privacy Policy is published within Orbit's website.

The Bluefin Risk Oversight Team has ultimate responsibility for ensuring that all staff comply fully with the relevant FSA and DPA legislation. Below is a summary of our practices in this area.

Data Protection Overview

We are registered as a Data Processor under the Data Protection Act 1998. We will endeavour at all times to have in place a level of security appropriate to the nature of the data which we process in relation to our clients and their employees and the harm that might result from a breach of security. The conditions are as follows:

- We must comply with the Data Protection Act. We will take no lesser steps to protect personal information about your company and employees than we would do to protect personal information about our clients for whom we are the 'data controller.' We will take appropriate technical and organisational measures to protect personal information from unauthorised or unlawful use, and against accidental loss, destruction or damage.
- If necessary, we will provide any information you may reasonably require in order to satisfy yourselves of the measures we are taking. We generally ask for such requests to be submitted in writing.
- We will only use personal information for the purposes of administering the benefits. We will not use it for any other purposes unless we are requested to do so by you, either verbally or in writing.
- All of our employees are given training on Data Protection, including the care and handling of personal information. Our staff code of conduct includes appropriate sanctions against the misuse of personal information.
- We will maintain the confidentiality of any personal or confidential information that you provide to us, or that is provided on your behalf. We will not disclose it to any third party without your consent, unless we are required to do so by law.
- If you receive a request for personal information from a member under section 7 of the Act (a subject access request), we will assist you as required in providing your response.

More generally, all our staff are completely aware of the need to retain absolute confidentiality on the content of their work. We achieve this through a framework of operational and compliance procedures and electronic system controls.

E-mail Security

We have not adopted the encryption of e-mails as a standard, as the majority of our clients are currently not able to interact with our systems on such a basis. We will work with a client to determine the appropriate standard, depending on their capability.

Once an e-mail is received into our organisation, we have controls in place to ensure that it is only available to relevant staff. These controls include restrictions on access to individual mail boxes and protocols on the archiving of e-mail.

All e-mail is captured at point of entry and a vanilla copy archived to preserve its integrity, for backup and legal disclosure requirements. Release from archive is subject to rigorous controls and has an appointed data custodian. This ensures total confidentiality and integrity of the e-mail system.

Data Confidentiality

Confidentiality of data is paramount to our business and we have adopted policies at a number of levels to address this. As well as physical and logical controls that restrict access to our system, we are mindful of our requirements under the Data Protection Act and have adopted policies to ensure that the data is secure:

- Users are only provided access to areas and systems that are deemed necessary for their job role.
- Users are set up by pro forma, which sets out the key systems to which access is required.
- Users are set up with the lowest level of security and the minimum access to data that is appropriate to their job. Higher security levels and access to other data will be granted only when deemed necessary to do so.
- Users are subject to our user password management protocol.
- There is an automatic password reset policy built into our Active Directory group policy. This requires users to reset their password every 45 days, with in-built constraints around password length and old password reuse.
- We have strict protocols in place around the use of portable devices for storing data and a suitable level of encryption for all portable applications.

Data Disposal

Underpinning the controls described above, the disposal of any information, whether paper-based, electronic, optical or magnetic media, is controlled under policy. We have a secure waste disposal contract covering paper based information and all electronic devices are disposed of in a controlled manner, with relevant certificates of disposal obtained.

Does your organisation have a documented information security policy?

We do have a documented information security policy. The following is a high level overview of our firm's security policy statement. The full statement is available upon request.

Introduction

The objective of this policy is to:

- Protect Bluefin's systems, data, network and equipment against loss, abuse or misuse.
- Make sure all users are aware of and comply with relevant legislation.

The aim is to ensure that:

- Regulatory and legislative requirements are met.
- Integrity of information and services is maintained.
- Availability of information and services is maintained.
- Information is protected against unauthorised access.

- Confidentiality of information is maintained.
- Business continuity plans are documented, kept up to date and tested regularly.

Compliance with Legislation

Bluefin must comply with all relevant UK and EU legislation. The two key pieces of legislation that cover IT security are the Data Protection Act 1998 and the Computer Misuse Act 1990.

The requirement for compliance rests with individual users, who may be held personally responsible for any breach of legislation.

Policy Awareness and Disciplinary Procedures

Staff are made aware of this policy which is published on Bluefin's intranet. Failure to comply with this policy may lead to the commencement of disciplinary procedures. Some elements of covering relevant legislation do stipulate that legal action can be taken.

Usage Monitoring

Staff are made aware that Bluefin has reserved the right to monitor the usage of any system, including specifically e-mail and internet usage. There is an e-mail and internet usage policy set out in the staff handbook, which is also available on the intranet.

Normally, monitoring will be limited to detecting the unauthorised use of systems, determining where usage is relevant to the company's business, preventing or detecting crime and ensuring effective use of systems.

Physical Building Security

Physical security of Orbit's office buildings are in-line with city based offices including security guards at the entrance of the building and ID pass controls on the doors.

The physical security at the hosting centre is of a very high standard. All personnel entering the hosting centre must be pre-booked, require photo identification and must be accompanied at all times.

Firewalls

Orbit's servers are protected by a pair of high-availability, fully Managed Firewalls (ICSA/IPSEC certified) provided by the security specialist Vistorm (BS7799 accredited).

Do you have formal personnel screening procedures to ensure that appropriate background / credit / reference checks are performed for all employees that have access to information processing facilities or otherwise handle customer information?

Yes. For all new joiners we use a third party identity verification company, Vero Screening, to carry out past employment checks, credit checks and qualifications, as well as obtain verification for any gaps in employment. The level of check varies according to the seniority of the employee and the role that they are being taken on to perform.

The procedures undertaken by Vero are contained within a commercial contract with Vero, which unfortunately we are unable to share. A copy of the form we ask new joiners to complete in order to commence the verification search is included. Programmes can be formulated either as a regular series of events, publications and on-line services, or on a much more ad hoc basis during the normal course of benefit provision. In either case we would expect that they will be reviewed regularly during formal governance meetings and service meetings with the employer.

Please describe your operational change control mechanisms for changes to information processing facilities and systems.

We use an application lifecycle management system, Surround SCM, to track all changes and requests.

Surround is a configuration management system which controls access to files and tracks changes over time. It combines the latest virtual branching technology with a detailed workflow system, enabling modelling of change processes and ensuring that these processes are followed each time a file is added or a change made. The system is ideally suited for parallel development environments, and provides inbuilt, robust version control protocols.

Flexible management reporting provides detailed accounts of who, when and what changed for each revision, enabling complete control of the software configuration management process and instant progress reporting.

Do you have controls in place to mitigate the risk of vulnerability to malicious software impacting your information processing facilities or operations?

Across Bluefin, all servers are protected by firewalls, IPs and DMZs. All office PCs are protected by anti-virus software, behind a corporate firewall and have strict permission management on them.

Orbit website infrastructure is hosted in secure facilities on hardened UNIX servers. Orbit's servers are protected by a pair of high availability Managed Firewalls, provided by Vistorm. The Managed Firewall Service is fully backed by a service level agreement.

Vistorm remotely monitor the Managed Firewalls 24/7, using the internet as the communications network. Their procedure is automatically to alert customers to any faults detected. Vistorm monitors the Managed Firewall from its Network Operations Centre using a mix of industry standard systems management tools and bespoke systems management software solutions developed by Vistorm themselves.

Vistorm provide the ongoing, full time operational management of the Managed Firewall. This includes the backup, restoration and general system maintenance, where applicable and appropriate, of all of the Managed Firewalls. Problem management facilities are provided on a continuous basis to nominated contacts, with no limits to the number of problems which can be raised. Problems are handled in accordance with a service level agreement. Vistorm also provide continuous ongoing comprehensive and authenticated change management.

From time to time vendors issue hot fixes, patches and upgrades to their software. Vistorm's Research and Development department review these releases within the context of the Managed Firewall Service and determine if they are relevant to Orbit and compatible with Vistorm's managed service architecture. This will include an assessment of the urgency with which these releases should be deployed if they are deemed relevant. Vistorm notifies Orbit if any changes are required or recommended. The decision to implement any hot fixes, patches or upgrades and the time at which they are implemented remains with Vistorm as part of the Managed Firewall Service. The provision of this service element is dependent upon the customer maintaining as current all applicable software subscriptions.

Qualys, a third-party company, is used to carry out monthly security tests on Orbit's infrastructure, which involve penetration tests and scans of the system. Vistorm perform a security audit every year or when a change to the application requires a re-audit. Results of these tests are confidential, but we would be very happy for you yourselves to scan the website if this would give you added confidence in our security.

Do you have formal process for managing user access to applications and systems that support customer information processing?

Fundamental to Orbit's on-line web application security is a requirement to authenticate each user and a system of authorisation to functionality specific to that user. The following processes summarise these security measures:

- Initial access to the application for each newly joining employee is through an invitation e-mail containing a system-generated user ID. When the employee takes up the invitation they receive a temporary password. This temporary password is valid for only 72 hours and the employee must confirm their date of birth as additional verification.
- Each user is then forced to change the temporary password when they first log on to the system.
- All passwords must be changed on a pre-defined, regular basis by each user.
- The user account is disabled if there are repeated incorrect attempts to log on. Re-activation can only be carried out by an administrator, who will verify identity by means of personal information questions.
- No data is retained on the user's computer, ensuring that it cannot be accessed by a third party.
- There is no third party access to Orbit's website.
- There are multiple levels of user authentication groups for the application, including super-user, employer and employee. Each level of user group has different, defined rights within the application, based on their unique log-in and password.
- Any Bluefin administrators who access company data go through a strict process when they leave service; one part of this is that their administrator access to the website is cancelled immediately. For client staff leaving the company, we would rely on the client to inform us when the employee is leaving, and would ensure that any administrator access is cancelled at the appropriate time.

Please describe the security mechanisms that you support for data transmission and storage, including data written to backup tapes and sent offsite.

All access to hosted servers is via a VPN. Access to consoles / shell is only supported by SSH.

Data transmission protocols are agreed with the third party during the implementation phase of all projects. We always recommend encrypted (Gnu)PGP data via sFTP or VPN.

Whenever an authentication or authorisation process fails or any other software fault occurs, does your platform deny access to protected resources?

Yes.

Do you store database and server credentials in a secure (non-public) location?

Yes. Server credentials are kept in a 2048 bit encrypted file stored on a file system, only accessible by the designated technical team. A written copy of the credentials is kept in a fireproof safe.

Does your platform encrypt passwords during authentication and in storage?

The Orbit application does not store passwords, only SHA-1 hash functions.

Does your platform log all security events processed by the application?

Yes. We have a transaction log that records all business transactions and an application log that stores all application transactions.

Does your platform encrypt confidential information in transit across public networks?

Server to server communications are made via SSH and certificate authentication. Information viewed over the network (ie by employees and employers using the website) requires HTTPS 1024 bit encryption. The site has also a Verisign certificate which authenticates who we are when someone access the site.

The encryption protocol for any bulk data feeds from clients (for example anything containing employee information) is negotiated with the client at outset, and will to depend to a large extent on the client's own encryption capabilities. However, we recommend that the data is encrypted via PGP encryption and that the information is transported using sFTP (SSH), a secure form of file transfer protocol using encryption.