



Hosting collaboration

Quality of service and 'project extranet' infrastructure

As well as seeking details about each online collaboration system and its supplier, clients should demand technical information about the infrastructure used by the supplier to host its technology, and corporate information indicating the strength and stability of organisation(s) providing this infrastructure to the supplier. This paper gives a BIW perspective on the key minimum quality of service (QoS) requirements for hosting a collaboration system.

Why you should read this document

In any business scenario, it pays to know who you are dealing with, but are the questions you need to ask always clear? The fast-moving collaboration technology market requires a careful approach extending beyond examination of the quality of the software and the calibre of the provider's management.

This paper outlines the key minimum quality of service (QoS) requirements for hosting a collaboration system, argues that managed hosting provides the lowest-risk solution (illustrated by a case study relating to BIW's hosting arrangements), and suggests some key questions where potential suppliers should be pressed to provide full information.

Contents

■ Why you should read this document	2
■ Contents	2
■ Avoiding risk	3
■ Quality of service	3
Minimum QoS requirements	3
DIY or outsource?	4
■ Managed hosting	5
■ The BIW case study: Attenda	6
Attenda: application-centric	6
Investing in security	7
■ Secure people to do business with	8
Attenda	9
■ Five key QoS questions	9
■ Further information	9

Avoiding risk

Within the UK architectural, engineering and construction (AEC) industry, online collaboration systems are becoming increasingly popular. Potential customers - whether they are clients, contractors, consultants or others - understandably want to know more about the different systems and their providers. However, in an industry renowned as risk-averse, the calibre of the provider's managers and the quality of their collaboration technology should not be the only consideration. Clients should also seek:

- technical information about the infrastructures used by the various suppliers to host the technology, and
- corporate information indicating the strength and stability of any third party organisation providing this infrastructure to the supplier.

This paper outlines the key minimum quality of service (QoS) requirements for hosting a collaboration system. It is vital that businesses undertake a methodical and impartial assessment of the facilities used to house their ICT systems. Without this, the business functions they perform will be subject to considerable yet avoidable risk.

Quality of service

Minimum QoS requirements

Depending upon the scale and sophistication of their technologies, service providers can deliver their systems in different ways. However, all should share the same basic quality of service requirements:

- high levels of performance (eg: speed of access to data)
- constant availability of application and data, 24 hours a day, 365 days a year, coupled with low latency (ie: minimal delay between sending data and recipient receiving it)
- high reliability and resilience (eg: full redundancy - all primary network system components such as servers, power sources and telecommunication links have secondary back-ups in case they fail)
- high levels of security, both physical (preventing unauthorised access to servers) and technological (preventing hackers, viruses, denial of service attacks, etc) , and
- service management to recognised standards of best practice (eg: the UK government-created ITIL, rapidly being adopted worldwide as the standard for best practice in IT service provision).

DIY or outsource?

How each provider meets these basic requirements will depend on the resources they have available and the importance they attach to each QoS requirement. The options facing UK clients and AEC organisations will usually reflect the locations of the servers used to manage the applications and their underlying data. For example, server(s) can be:

- housed in the office(s) of the project client or other member(s) of the project team
- managed in the application provider's own facility
- located in data centre run by an internet service provider (ISP) - options include: sharing a server with other (sometimes competing) applications and/or websites; a dedicated server leased from the ISP; and co-location - the provider places its own server, set up with all the software, in the ISP's facility
- managed at a specialist hosting / data centre

In delivering business-critical web services, particularly those involved in delivering and then managing multi-million pound capital assets, users need a lowest-risk solution.

First, few in-house ICT departments have the technical facilities, resources, skills and experience needed to deliver a service that would meet AEC clients' minimum QoS requirements (Do they currently provide responsive, timely support and guaranteed uptime on all hardware, software and network functionalities? If so, are such undertakings backed up by service level agreements?)

Second, while some providers may have developed an infrastructure eminently suited to continued research and development of their service technologies, this development environment will almost certainly not be suitable for delivering them (this, of course, assumes that the service provider makes direct inputs into the continued development of their services - some providers simply re-sell third party technologies). Moreover, creating a parallel service delivery infrastructure would dilute the business's focus on creating, implementing and supporting customer-focused, industry-strength software.¹

Third, some ISPs may not provide pure internet protocol (IP) networks; their communications links may segment into other services, such as voice or fax, so that project data has to share bandwidth with non-IP traffic, compromising quality and reliability. It should also be noted that the networks of ISPs who host public dial-up operations are subject to massive load fluctuations; by contrast, networks able to provide hosted applications with dedicated bandwidth 24x7 will be capable of routing very high volumes of traffic at consistently high data rates.

In delivering business-critical web services, particularly those involved in delivering and then managing multi-million pound capital assets, users need a lowest-risk solution.

¹ BIW white paper 'Software as a service' details the customer benefits of using applications delivered via 'wave two' application service providers or business service providers (BSPs).

Fourth, even with stringent service level agreements, conventional website hosting arrangements are often not as resilient or responsive as the ultimate customers' minimum QoS requirements. Many ISPs concentrate on selling network bandwidth capacity on their global networks, and providing power and rack space in their expensive, state-of-the-art data centres. As a result, they try to manage a mixture of hardware systems (eg: Dell, IBM, Hewlett-Packard, etc), running a multitude of operating systems (a bit of Microsoft here, some Unix there, some Linux over there), juggling bandwidth and compromising as they try to reconcile the competing needs of website owners, service providers, etc.

Fifth (and following on from the point above), however sophisticated the data centre, hardware and software, it still needs careful, expert management by certified professional staff 24x7 – people who, ideally, specialise in a small number of hardware platforms and operating systems. After all, it is these people that must devise, implement and adhere to the procedures that underpin the integrity and security of the system.

Finally, a concentration on the hardware, power, connectivity and infrastructure management issues of hosting also obscures the most volatile part of the whole hosting solution: the web application itself. Truly efficient hosting of collaboration technologies requires proactive anticipation, monitoring and management of the ongoing demands made on that infrastructure by the hosted applications.

Clearly, then, there are potentially serious drawbacks with services that may rely on self-hosting, reliance on the service provider's own servers, or on use of a conventional ISP. Recognising that customers' key QoS requirements involved non-core skills and expertise that complemented its own abilities, BIW sought a 'managed hosting' partner.

Truly efficient hosting of collaboration technologies requires proactive anticipation, monitoring and management of the ongoing demands made on that infrastructure by the hosted applications.

Managed hosting

A managed host procures, configures, installs and maintains the necessary servers, firewalls and other devices that its customer's software architecture requires. Once configured, the host then provides dedicated bandwidth for its customer's applications, and connects the servers to the web via its own network, where the application is constantly monitored to ensure availability and optimal performance. (This may appear the most costly hosting option, but efficiency and security are vital where multi-million pound capital projects are dependent on a business-critical web service.)

Normally, a managed host's customer does not get involved in the maintenance of the hardware, but is able to take advantage of the host's processes and experience to implement, maintain and update services in less time and with higher reliability than other hosting methods. Moreover, managed hosting ensures technology services remain easily and seamlessly scalable. This is vital as the user base grows, as demand for bandwidth increases, as the applications are upgraded, etc.

A managed host's customer does not get involved in the maintenance of the hardware, but is able to take advantage of the host's processes and experience to implement, maintain and update services in less time and with higher reliability than other hosting methods.

In short, the 'managed hosting' provider should easily be able to exceed the client's minimum QoS requirements regarding all the infrastructure issues integral to 24x7 hosting of applications, eg:

- exclusive use of 'best in class' server hardware and software, for both primary and secondary systems
- partnerships with several telecommunications businesses ('telcos') to provide pure IP-routed access to internet backbone, plus secondary backbone connections
- peering arrangements with each telco to ensure data centre traffic is prioritised (peering is the process of linking one telco's backbone network to another's to allow traffic to travel across the networks)
- guaranteed, dedicated IP bandwidth, measurement and scaling
- router(s) and other communication equipment connecting server(s) to the internet, plus back-up connections
- firewall(s) and other security hardware and applications
- racks, cabling and server-friendly facilities
- uninterruptible power supply and back-up generators
- high-calibre infrastructure managers, working to accredited information and IT management standards (eg ISO/IEC27001:2005 and ITIL)
- specialist in-depth expertise on specified hardware and software platforms
- database back-up, maintenance and recovery
- remote application monitoring and support
- capacity management and planning
- change management

The BIW case study: Attenda

Attenda: application-centric

BIW's partner is Europe's leading infrastructure management company, Attenda, which offers a complete turnkey web operations service² that frees BIW developers or in-house technical staff from routine operational tasks. As a result, they can focus on their core role of creating, implementing and supporting BIW's industry-strength software applications.

² More technical details about the infrastructure provided by Attenda to host BIW's services are available in the BIW technology paper "Hosting BIW".

Realising that the most volatile part of any hosting solution is the application, Attenda's engineers have a deep understanding of BIW's collaboration technology, its commercial purpose and technical functions. They have devised and applied a tailored plan to monitor deep into the applications; escalation routes have been pre-agreed for use in the event alerts are generated; as a result, Attenda can manage availability problems quickly and effectively. Its sole agenda is to maximise the availability of the application - not solution components like bandwidth, rack space or power.

Attenda's monitoring recognises that to successfully return content or data, or complete a transaction for a BIW user, every aspect of the application and its infrastructure must correctly operate in sequence. Attenda proactively monitors BIW applications to ensure that:

- the sites are always on-line (remote/user experience monitoring)
- the various elements within the infrastructure are delivering the service they were designed to provide (service/application monitoring)
- there are no hardware or operating system faults or server performance/maintenance issues (hardware/OS monitoring), and
- there are no intruders trying to get into the system illegally.

It is this integrated monitoring that differentiates the BIW service from other similar offerings, meaning BIW can offer its clients a high quality service that is secure, resilient, responsive and reliable.

Attenda's proactive, integrated monitoring differentiates the BIW service from other similar offerings, meaning BIW can offer its clients a high quality service that is secure, resilient, responsive and reliable.

Investing in security

"Information is the lifeblood of today's business, underpinning day-to-day operations and facilitating effective decision-making. Increasingly, access to the right information by the right people is vital to gaining competitive advantage or simply remaining in business. To provide this access, businesses need to understand the associated risks and put in place appropriate counter-measures."

(Information Security Breaches Survey 2002, PriceWaterhouseCoopers and DTI)

It is dangerous to under-estimate security issues. A 2001 Communications Management Association survey of IT professionals indicated that one in three UK businesses had been the victim of a major security break in; the 2002 PWC/DTI survey put the figure higher, at 44%. Almost half said that the future of their organisation could be ruined by a serious hacker attack. Of 167 participants in a one-month BBC experiment in 2001, 159 were subject to hack attempts. Over 1700 hack attempts were made, with one participant subject to 91 separate attacks. Attenda constantly monitors intrusion attempts, and its experience suggests that a network will typically face approximately 35,000 virus attacks or attempted hacks every day (in one experiment, an unguarded server was hacked within two hours of being connected to the internet!).

One in three UK businesses have been the victim of a major IT security break in. ... Attenda's experience suggests that a network will typically face approximately 35,000 virus attacks or attempted hacks every day.

The BIW service is very secure. Attenda is certified to the ISO/IEC27001:2005 standard for information management security. According to Simon Hansford, vice-president of platform and products at Attenda: "This requires, amongst other things, that businesses implement change control and business continuity plans, making websites more robust and protecting them from potential threats to availability. Companies need to either have an in-house team dedicated to making this practice a reality, or work with a partner that can provide the necessary expertise and time to pre-empt disasters before they happen."

Attenda also believes that internet-focused IT initiatives demand the same service management standards as traditional functions, such as payroll and accounts. Yet over 80% of UK companies do not adhere to government best practice guidelines for operating IT systems, putting businesses at risk of downtime, brand damage and loss of revenue, and preventing effective communication with partners/suppliers. Research commissioned by Attenda in 2001 showed that just 10% of companies adhered to government ITIL (IT Infrastructure Library) standards, and only 18% of those who outsource checked that partners adhered to ITIL standards. Mark Fowle, CEO at Attenda said: "Insisting upon these standards would allow organisations to properly assess the quality of service offered by co-location, managed hosting and outsourced internet operations providers. This will help businesses to choose suppliers on the basis of what they do, rather than what they say they do."

Secure people to do business with

As well as understanding how secure a service provider's infrastructure is, it is vital to establish that the company providing the infrastructure is itself stable and secure.

During the early boom years of the internet, many companies - including several major telecommunications businesses - were falling over themselves to join the market and build new data centres to handle the anticipated demand for ASP and website hosting capacity. But when the 'dot.com bubble' burst in 2000, those market forecasts proved to be over-optimistic, and the building binge created a glut of under-used data centre space in many regions. Simultaneously, customers became more discerning, shifting away from co-location of their servers towards managed hosting. As a result, co-location data centre space became a commodity, with pressure to keep prices low in order to compete in a buyer's market. Sales have also fallen at a time when it is even more expensive to transform a co-location ISP into a managed hosting provider. In an overcrowded market, many data centre owners, including some telcos, have experienced significant problems.

For example, in September 2001, Exodus Communications (an American corporation whose UK facilities hosted some UK collaboration systems) applied for protection under Chapter 11 of the US Bankruptcy Code. By the end of February 2002, a substantial portion of its business and assets, including those in the UK, was sold to Cable & Wireless plc. Similarly, ISPs such as Energis and PSINet also faced financial troubles, with PSINet folding in early 2001.

Attenda

By contrast, Attenda was established from the outset to add value by focusing purely on providing high application availability. It does not build or physically manage data centres or networks, nor does it design applications. Some of Europe's most successful companies already entrust mission-critical applications (as opposed to public 'brochureware' websites) to Attenda, including Avis Europe, bmi, easyCar, Compass Group, Microsoft, NHS, Princes, Travelodge and Sun Microsystems. The company has ranked in the *Sunday Times* Tech Track 100 list for three consecutive years, and has substantial financial backing from Phoenix Equity Partners, UBS Capital, Tarrant Venture Partners and Compaq Computer Corporation.

Five key QoS questions

1. Is the collaboration system provider able to guarantee system and data availability and high levels of performance, backed by demanding service level agreements?
2. Is the service hosted on a scalable infrastructure in which all power, internet backbone connections and network components have secondary back-ups in case of failure?
3. Is the hosting infrastructure created using 'best in class' server hardware and software components from single vendors (eg: Compaq, Cisco, Microsoft)?
4. Is the hosting infrastructure managed 24x7 by specialists working to systems which carry ISO/IEC27001:2005 certification for secure information management?
5. Is the service hosted by a conventional ISP or by a dedicated total managed hosting provider working to ITIL service management standards?

Further information

- *For more technical details about the infrastructure provided by Attenda to host BIW's services, ask for the BIW technical paper "Hosting BIW".*