



## Legal issues in collaboration

### Understanding contracts, licences, etc

The technical merits of an online collaboration system are clear; there are no issues regarding the strength and stability of the provider; and the provider's hosting resources meet the customer's minimum quality of service requirements. But if something goes wrong, what legal recourse does the customer or the end user have against the technology provider? In a relatively young market without standard contracts or licences, it is vital to ensure that risks and liabilities are shared equitably between the provider and the customer and/or the project team users.

Although illustrated by examples showing how BIW Technologies has tackled some of the key issues, this paper aims to set out the key issues to be addressed regardless of the identity of the service provider.

## Why should you read this white paper?

As online collaboration systems become more widely used in the UK architectural, engineering and construction (AEC) industry, customers need to be aware of the key legal issues surrounding their use. This paper looks at some of the major areas of concern, including:

- the legal status of electronic communications
- the legal relationship with the software vendor
- service interruption or unforeseen termination

Although it is illustrated by examples showing how BIW Technologies has tackled some of the key issues, this paper aims to set out the key issues to be addressed regardless of the identity of the software vendor.

NB: this paper gives only general observations on legal issues and is not intended to provide specific advice. Where appropriate, readers are recommended to seek guidance from their own professional legal advisors.

## Contents

■ Why should you read this white paper?	2
■ Contents	2
■ Executive overview	3
■ Introduction	4
■ Legal status of electronic communications	4
Contract provisions regarding electronic communications	4
Legal admissibility of electronic communications	6
■ Legal relationships with the ASP	8
Master Licence Agreement (MLA)	8
End User Licence Agreement (EULA)	9
Service level schedules / service level agreements (SLAs)	10
Project protocol documents	11
■ Service interruption or unforeseen termination	12
Risk of data being corrupted or lost	12
Managing service interruptions	12
Managing ASP termination	13
Early warning	14
Escrow arrangements	15
■ For further information	15
Useful web resources	15
Publications	15

## Executive overview

---

This white paper gives an overview of some key legal issues. The following checklist of questions indicates the key areas that BIW believes should be covered by any organisation contemplating a customer relationship with a software vendor offering web-based collaboration services, particularly if the vendor is also responsible for hosting the application and data:

- Does the vendor demonstrate awareness of the five principles of information management underpinning legal admissibility?
- Is the vendor's hosting infrastructure compliant with relevant British or international standards? More specifically, is it certified under parts of the standards which require regular audits?
- Does the vendor's standard customer agreement (ie: Master Licence Agreement) cover all key areas?
- Is the vendor's insurance cover adequate?
- Is the End User Licence Agreement (EULA) likely to be acceptable to all members of the supply chain?
- Is there a proper process for making the EULA binding between all members of the supply chain and the vendor (not just a "click through")?
- Is the vendor generally using well-drafted agreements? (Poor documents may expose the vendor to the risk of crippling legal action, and invalidated insurance cover, if it was to be sued by another, perhaps larger client.)
- Does the ASP provide and develop a tailored Project Protocol Document that enables all members of the project team to understand their roles and responsibilities?
- Is there a clear and comprehensive Service Level Agreement covering all key areas of service delivery and availability?
- Has the vendor outlined procedures in case of temporary interruption to its service?
- Is the vendor willing to share information about its financial situation, insurance cover and shareholder details and structure (subject to a non-disclosure agreement, if necessary)?
- Is project data guaranteed to be capable of being produced (or transferred) in an industry standard format (eg: XML)?
- Does the vendor offer any contingency arrangement that extends service availability beyond cessation of company operations?
- Does the vendor offer a third party escrow arrangement?

## Introduction

---

Online collaboration systems are becoming widely used in significant projects in the UK architectural, engineering and construction (AEC) industry. In deciding which one to use, customers should research the different systems and their vendors (sometimes called Software-as-a-Service (SaaS) or On-demand software vendors, or application service providers, ASPs), and should assess:

- the strength and stability of the vendor's business, including the calibre of its management
- the quality of the collaboration technology, its service features and the potential 'fit' with the customer's future needs
- technical information about the vendor's hosting infrastructure<sup>1</sup>
- corporate information indicating the strength and stability of any third party organisation providing this infrastructure to the vendor.

However, while customers' and project teams' enthusiasm for the technology has grown rapidly, and there have been significant advances in the technical capabilities of the leading systems, there has been much slower progress with respect to legal issues. The AEC industry is notoriously risk-averse and legal issues have hampered rapid introduction of such information and communication technologies (ICT).<sup>2</sup> Articles in industry publications<sup>3</sup> have tended to highlight two or three areas of particular legal concern, including:

- the legal status of electronic communications
- the legal relationship with the vendor
- service interruption or unforeseen termination

## Legal status of electronic communications

---

Broadly, the same legal principles apply whether parties communicate on paper or electronically. Paper-based records (documents, drawings, etc) are simply records kept in a particular medium, and electronic media are no less valid. But it is important to ensure that records are authentic, accurate and accessible.

## Contract provisions regarding electronic communications

Although the use of electronic media to exchange information within the AEC industry has become more widespread (from email, through floppy disks and CD-ROMs, to FTP sites and now project extranets) in recent years, questions about the legal admissibility of electronic communications have led some AEC professionals to delay decisions about using online collaboration systems.

---

<sup>1</sup> This and the following point assumes the solution is not being hosted by a member of the project team.

<sup>2</sup> Peter Goodwin (2001) *Effective Integration of IT in Construction*, Building Centre Trust, London

<sup>3</sup> For example: 'Stung', *Construction Manager*, September 2001, pp.8-10; 'The ASP with a sting in its tail', *Building*, 8 June 2002, pp.50-51; 'Wired up', *Building*, 2 December 2005.

This uncertainty was compounded by the absence of appropriate provisions in many standard formal contracts. Few contracts made any explicit reference to the possible use of modern ICT, important communications were assumed to be delivered 'in writing' in a tangible, paper-based form, such as by letter, or by the issue of drawings.

Many construction contracts require participants to issue formal notices, but are not always clear about how such notices shall be given and whether electronic communications will suffice. In a presentation to industry professionals at the ICE in London in December 2001, solicitor Ed White of Masons highlighted the relevant clauses of several standard contracts:

*JCT*

*Where the contract does not specifically state the manner of giving such notices, such notices shall be given or served by any effective means to any agreed address*

*Engineering and Construction Contract*

- 13.1 *Each instruction, certificate, submission, proposal, record, acceptance, notification and reply which this contract requires is communicated in a form which can be read, copied and recorded*
- 13.2 *A communication has effect when it is received at the last address notified by the recipient for receiving communications or, if none is notified, at the address of the recipient stated in the Contract Data*

*FIDIC*

- 1.3 *... in writing and delivered by hand (against receipt), sent by mail or courier, or transmitted using any of the agreed systems of electronic transmission as stated in the Appendix to Tender...*

It was Masons' opinion that the first two contracts needed amendment to be appropriate for projects where any online collaboration system was employed. Masons cited with approval some sample clauses from a retailer's contracts:

- 1.1 *"Writing" includes e-mail, facsimile transmission and/or communication in another durable medium that is available and accessible*
- 2.1 *Any communication sent electronically by e-mail or otherwise:*
  - 2.1.1 *Will be deemed to have been sent once it enters an information system outside the control of the originator of the message;*
  - 2.1.2 *Will be deemed to have been received by the intended recipient at the time that in a readable form it enters an information system that is capable of access by the intended recipient.*

A BIW white paper "The role of electronic information in construction contracts" written by solicitors Hammond Suddards Edge,<sup>4</sup> outlines standards and rules that can be applied to facilitate the use of electronic communications:

- UK Standard Interchange Agreement<sup>5</sup> - provides a standard protocol for use by parties who wish to communicate electronically. It mainly concerns security, such as authenticity and integrity of data, when it was received and how data logs should be stored and maintained. The Joint Contracts Tribunal provides, as an option, for the provisions of the Standard Interchange Agreement to be incorporated into construction contracts based upon the JCT's standard form. Where the option is chosen, the contract provides that any communication that must be in writing will be validly exchanged when sent electronically.
- Electronic Communications Act 2000 (and the EU Directive on E-commerce) - created a legal framework for the use of electronic signatures so that people can be sure about the origin and integrity of electronic communications. Its provisions were extended incrementally<sup>6</sup> to existing legislation that had required certain documents to be in writing.

It should be noted, however, that electronic signatures are rarely required in project collaboration systems.

### Legal admissibility of electronic communications

Masons' Ed White addressed the issue of legal admissibility by reference to the Civil Evidence Act 1995:

*"Where a statement contained in a document is admissible as evidence in civil proceedings, it may be proved:*

- (a) by the production of that document, or*
- (b) Whether or not that document is still in existence, by the production of a copy of that document or the material part of it, authenticated in such a manner as the Court may approve."*

It is therefore important that a party using electronic information in the courtroom has a rigorous audit trail reliably logging when a drawing or document was created, every instance when it is sent or received, and if it has been amended (and if so, when and by whom). The court may need to understand how the original was turned into an electronic image stored in the system, then sent and received without alteration, up to and including its production in court.

Arguments over admissibility of evidence can lead to investigations into the system that produced the paper, the method of storage, operation and access control, and even to the computer programs and source code. It may also be necessary to satisfy the court that the information is stored in a "proper" manner.

---

<sup>4</sup> Copy available from BIW on request.

<sup>5</sup> Developed by the Electronic Commerce Association (formerly the EDI Association), now known as GS1 UK.

<sup>6</sup> The main body of the regulations implementing the EU E-Commerce Directive came into effect on 21 August 2002.

Both Masons and Hammond Suddards Edge agree that the ability to show that an electronic information system is managed in accordance with internationally recognised and audited codes of practice or standards - such as ISO/IEC27001: 2005 (formerly BS7799/ISO 17799) - will be persuasive to a court of law. BSI codes of practice such as PD0008: 1999<sup>7</sup>, PD5000: 1999<sup>8</sup> and PD0010: 1997<sup>9</sup> also provide guidance (though BSI also notes: "implementing the code does not guarantee legal admissibility, as this status can only be confirmed by a Court of Law"<sup>10</sup>). Customers should expect a vendor to have addressed the five principles of information management set out in PD0010:

- information management - information types need to be identified and their different management requirements (eg: security, format, retention, etc) understood
- duty of care - demonstrating a responsible approach to legislative and regulatory requirements - evidenced, for example, by compliance with ISO/IEC27001: 2005 (*see below*)
- documented procedures - business processes and procedures (eg: date/time stamping, version control, authentication, back-up, maintenance, etc) need to be identified, specified and applied, and will cover both software and hardware issues. Again, compliance with best practice guidelines, eg: the UK government ITIL (IT Infrastructure Library) standards, would be a persuasive factor
- enabling technologies - component technologies (eg: access control mechanisms, storage media, data integrity, compression techniques, etc) need to be identified, specified and documented
- audit trails - can the system permanently and securely log details of each significant event in the life of a piece of information?

... the ability to show that an electronic information system is managed in accordance with internationally recognised and audited codes of practice or standards - such as ISO/IEC27001: 2005 - will be persuasive to a court of law.

ISO/IEC 27001:2005 superceded BS7799. Part one of British Standard BS7799 (international standard ISO 17799 was based on the British Standard) laid down basic principles of information security management and set out the code of practice to be followed by those managing electronic data. Part two, the Information Security Management System (ISMS), covered certification processes to ensure compliance with part one and could have an important positive influence in determining the authenticity and accuracy of electronic documents that are submitted as evidence. The wider-ranging and more exacting international standard, ISO/IEC27001, was introduced on 15 October 2005.

#### BIW hosting

BIW's hosting partner Attenda was one of the first UK companies to be certified against BS7799 part 2, and then one of the first to be certified by BSI as compliant with ISO/IEC27001:2005 (on 10 January 2006). With all BIW users' interactions with the collaboration system being completely managed via Attenda's infrastructure, this means BIW's collaboration platform is the first - and so far only - 'extranet' system managed on a system certified to ISO/IEC27001:2005.

<sup>7</sup> Code of Practice for Legal Admissibility and Evidential Weight of Information Stored Electronically

<sup>8</sup> Electronic Documents and E-Commerce Transactions as Legally admissible Evidence

<sup>9</sup> The Principles of Good Practice for Information Management

<sup>10</sup> www.bsi-global.com

## Legal relationships with the software vendor<sup>11</sup>

Especially where the vendor is responsible for hosting the collaboration system, managing the information created by a project team places some strong obligations on the software vendor. It is vital that appropriate legal arrangements are put in place to support the relationships:

- between a vendor and a customer (or the customer's agent, eg: a construction manager). This may involve a Master Licence Agreement (also known as an ASP Agreement).
- between a vendor and end-users (ie: project team members) of the vendor's technology. Typically, this involves an End User Licence Agreement or some form of standard Terms and Conditions<sup>12</sup>, sometimes viewed on-screen when the application is first used.<sup>13</sup>

It may also be useful to specify relationships:

- between individual project team members stipulating use of the vendor's technology to communicate with each other. This may simply require amendments to consultant agreements and/or contracts with the main contractor and sub-contractors (*see pp. 4-6*), or may be covered in specific project protocol documents (*see p. 17*).

The nature of these relationships will, of course, vary according to the different vendor charging structures.

### Master Licence Agreement (MLA)

The MLA covers the relationship between the vendor and the ultimate customer (or its agent). The areas covered should include:

- grant of a non-transferable non-exclusive customer licence to access and use the collaboration service in relation to its project(s)/business
- restrictions on the use of the collaboration system (eg: posting information that is illegal, defamatory, indecent, etc; spreading software viruses; spamming, etc)
- clarification of the parameters governing use of project data by authorised project participants only (including relevant vendor staff)
- terms whereby nominated participants will enter into an appropriate end-user licence agreement with the vendor

<sup>11</sup> BIW white paper "Confidentiality, copyright and security" (available on request from BIW) covers some of these issues in greater depth.

<sup>12</sup> Customers need to ensure that the terms and conditions of the End User Licence Agreement with the vendor are appropriate and reasonable so that all members of their supply chain will be content to sign the EULA. If the EULA is not accepted by all supply chain members, gaps will arise in the chain of liabilities.

<sup>13</sup> It may not be adequate for an individual to simply click-through an on-screen EULA; if a dispute arises, it may be necessary to ascertain the identity and the authority of the person to enter into that Agreement on behalf of the supplier. Accordingly, a vendor may insist on a copy of the EULA signed by an authorised signatory.

- payment terms
- copyright of the vendor's collaboration technology
- vendor use of the customer's branding and data
- indemnification of the vendor against misuse, unauthorised use, etc, of the collaboration system
- confidentiality, including security precautions with respect to user names, passwords, etc
- termination provisions (including what may happen to the data once the project is complete)
- jurisdiction (eg: agreement written in accordance with English law; English courts to have non-exclusive jurisdiction)
- limitation of vendor liabilities

### End User Licence Agreement (EULA)

An EULA will describe the contractual relationship between a project's participants and the vendor. In many key respects, it will reflect conditions imposed in the MLA (*see above*), but at a level specific to participants. For example:

- the participant's licence to access and use the collaboration system in relation to their role on particular project(s) and/or for customer(s)
- terms whereby this licence might be terminated (eg: if the client relationship with the participant is discontinued)
- grant of a licence to the vendor to store and, subject to access privileges, to access and view project-related information where the participant owns the intellectual property rights

Client contracts with designers usually include provisions about copyright in the designer's designs; typically, the designer retains the copyright but grants a licence to the client and other team members to use the design in relation to the specific project. The EULA should reflect this principle, extending the licence to include viewing rights for the vendor.

The MLA and/or the EULA will normally seek to limit the vendor's liabilities for direct and indirect/consequential damages. Customers and/or end-users should check such agreements carefully to ensure that they are well-drafted and that the vendor is not avoiding liability unreasonably - for example, it may omit liability for, say, loss of data due to its own negligence, non-deliberate action, system non-availability, under-performance, or inaction, or it may limit liability to a small sum of money out of all proportion to the actual impact of any loss<sup>14</sup>.

---

<sup>14</sup> Note: the validity and enforceability of such clauses in a vendor's standard terms is controlled by the Unfair Contract Terms Act 1977. See also, for example, *St Albans City and District Council v International Computers Ltd* [1996] 4 All ER 481.

Customers should also be careful to ascertain that a vendor is adequately insured; can the vendor meet its liabilities if sued by the customer? Moreover, if a vendor is sued by another - perhaps larger - customer (particularly if a court found that its liability limit was unreasonable), does the business carry sufficient cover to ensure that it can continue to deliver its services?

Complementary information to the Master Licence Agreement and/or the End User Licence Agreement may be contained in separate documents (but forming part of the contract), including schedules outlining agreed levels of service delivery, and project protocol documents.

### Service level schedules / service level agreements (SLAs)

If the vendor outsources its hosting infrastructure, the specified service delivery levels will typically reflect the service level agreements (SLAs) between the vendor and its hosting infrastructure provider; otherwise, the vendor may specify a SLA direct with the customer reflecting its own capabilities. Sometimes described as the bedrock of contractual relationships with SaaS vendors, SLAs specify how the service will be delivered. They should include specifications relating to:

- provision of a secure system (including: firewalls, intruder and virus protection, etc)
- provision of appropriate back-up systems
- compliance with the stated functionality
- ensuring the integrity of data processed and stored on the system
- creation of a full audit trail of the project (including storage of all current and prior versions of documents and information along with related comments, 'red-lines', 'mark-ups' and associated data, eg: 'action by' dates, 'reason for issue', 'instructions', etc)
- provision of useful access to the full audit trail (eg: a searchable database created and delivered from within the system)
- ensuring the identity of each user (eg: via entry of a password and username - but users will still be responsible for ensuring the security of their individual details)
- provision of appropriate user access rights to access and view particular documents
- sufficient levels of processor, system memory, disk space and telecoms bandwidth availability to allow adequate performance (eg: response times when users interact with the software)
- levels of system availability (such as 99 per cent during working hours - but allowing for occasional, planned (ie: notified in advance) equipment or software upgrades) downtime
- provision for upgrades to latest software versions, and guarantee of continued compatibility of existing data with new functionality

- clearly specified levels of customer support (eg: helpdesk), perhaps defining response times, severity levels, etc
- extent and quality of end-user training

Interestingly, an in-house ICT department is unlikely to have an SLA with its captive user base. So, one benefit of outsourcing to a SaaS vendor is that it can introduce a degree of certainty to ICT delivery that simply did not exist before.

What is covered in a SLA is open to negotiation between a customer and the vendor, and different vendors will, of course, have different capabilities with respect to the various key areas covered by a SLA. Within a project team, users may also have some experience in working with different vendors' systems and customers may wish to consider user preferences when it comes to assessing SLA specifications.

... an in-house ICT department is unlikely to have an SLA with its captive user base. So, one benefit of outsourcing to a SaaS vendor is that it can introduce a degree of certainty to ICT delivery that simply did not exist before.

For example, a vendor might stipulate: "the system is not available between 4.00 and 6.00am daily, or as notified from time to time". Customers need to beware of such imprecise definitions, particularly if there is no guidance on: (a) how much advance notification will be given, (b) how the notification will be delivered to the customer and/or end users, and (c) how long such periods of non-availability might typically last. Prolonged or frequent periods of non-availability can also adversely affect efficient use of the collaboration system.

#### Round-the-clock working

In BIW's experience, a project extranet is often used round-the-clock. Monitoring its system in one 24-hour period, BIW found the first user login was made at 04.13am, the last at 23.21pm. A project may have a multi-national team, or have stakeholders who travel to different time-zones, and limitations on system availability could impact on such users.

### Project protocol documents

Part of the standard implementation service offered by a vendor should cover the provision and tailored development of a Project Protocol Document setting out the standards or rules of operation for user companies working on collaboration systems. Typically, they will:

- provide common protocols describing how users publish, retrieve and manage information quickly and efficiently
- be modified by the customer (or its agent) to suit its processes
- as a 'live' document, be maintained and updated as required by the customer (or agent)
- need to be read in conjunction with non-project-specific guides on use of the collaboration system (eg: user guides, etc)
- detail the pragmatic working procedures to be followed by participants during any temporary suspension of service (such procedures are essential to ensure the integrity of the data once the service recommences - *see also pp. 12-13*).

## Service interruption or unforeseen termination

### Risk of data being corrupted or lost

Many people fall into the trap of believing that electronic communications are less secure than traditional forms of communication. In fact, electronic exchange of information is often intrinsically more secure than, say, exchange of paper-based information.

For example, members of AEC project teams have traditionally communicated by committing their ideas to paper; this flammable material was then put into an envelope made of the same material, and then dropped into a post-box to be looked after by an outside organisation. After being handled by unknown people and machines, the envelope and its contents were bundled up indiscriminately with numerous other items before being delivered (hopefully!) to the correct location and then distributed to the right recipient.

(Even then, if it transpires that the document has not been read or has been read by someone who did not appreciate its significance, then that is a matter for the recipient. It cannot be said that the sender is at fault in any way.)<sup>15</sup>

Electronic exchange of information, by contrast, offers:

- audit trails showing who has seen or amended the information and when
- automatic recording of publication and distribution of information
- automatic recording of receipt of information
- information management by an organisation with whom the customer and participants have contractual relationships, and
- verification checks to ensure that information received is identical to that which was sent.

### Managing service interruptions

A SaaS vendor can take considerable steps to ensure that its service infrastructure is as robust and resilient as possible. For example, it can ensure high levels of redundancy (in this context, 'redundancy' refers to the availability of secondary, stand-by or back-up systems that can be made instantly available if a primary system develops a fault), so that no single point of failure exists.<sup>16</sup>

... electronic exchange of information is often intrinsically more secure than, say, exchange of paper-based information.

A SaaS vendor can take considerable steps to ensure that its service infrastructure is as robust and resilient as possible. For example, it can ensure high levels of redundancy ... so that no single point of failure exists.

<sup>15</sup> Thorneycroft, Ben (2007), 'Is service by fax or email legally binding?' *Contract Journal*, 14 March 2007, p.35.

<sup>16</sup> BIW has a white paper 'Hosting collaboration' and a technology paper 'A lowest-risk solution: the BIW hosting infrastructure,' both available on request from BIW.

Nonetheless, no technology is infallible. As solicitors Gillian Birkby and Jon Nugent (from Mayer Brown Rowe & Maw) suggest<sup>17</sup>, customers and users need to be clear about what happens if/when a project extranet system crashes:

*“If the system crashes, there must be a back-up system that enables each of the participants - designer, contractor, subcontractor, client, to carry on working with minimal delay to design or progress on site. This may mean that whenever a document is uploaded onto the network, the person who has created or amended the document keeps a copy in their own electronic file, so it is available if needed. Everyone will, of course, revert to emails and faxes and circulation of hard-copy drawings until the system is back up and running, but there must be a procedure for updating the extranet as soon as it is back on line, so that everyone can have confidence in continuing to use it, and not resort to their own back-up system.*

*“This is normally achieved by devising a series of rules for the operation of the extranet, sometimes called a protocol, which becomes one of the contract documents for each of the organisations working on the project.”*

Different vendors may handle this issue in different ways, but one solution is to rely on email until the collaboration system is operational again. Clearly, if the integrity of the single central repository for all project data is not to be compromised, some back-up processes need to be specified.

#### Managing a temporary service interruption

BIW's project protocol documents nominate a 'Project Information Coordinator' (PIC) who assumes additional responsibilities should the collaboration system stop working temporarily. To avoid confusion and duplication of effort when publishing, for example, all emails and relevant attachments should be sent to the PIC and it will be his/her task to input drawings, documents, comments, requests for information, instructions, etc once the collaboration system is reinstated.

### Managing service termination

Given the relative immaturity of the UK collaboration service market and the number of vendors competing for market share, lawyers have understandably warned customers to take steps to cater for the possibility that a chosen vendor may become insolvent. Birkby and Nugent suggest that the contract with the vendor should provide:

- *“A right to terminate a contract and transfer to an alternative service provider in the event of any doubts about the ASP's ability to continue providing services;*
- *“An obligation on the ASP to provide assistance on transfer of the service to an alternative ASP, by providing access to all necessary records and data. Assistance in the form of consultancy services may also be required; and*

<sup>17</sup> 'The ASP with a sting in its tail', *Building*, 8 June 2002, pp.50-51

- *“An obligation to make records available in specified formats that can be accessed by the ASP’s customer.”*

### Early warning

Birkby and Nugent urge prospective customers to monitor the financial status of their service providers so that they get early warning of any problems:

*“... insolvency of the ASP would be likely to cause serious problems and realistically, many provisions will become impossible to enforce in the actual event. So you may also wish to require the ASP to provide regular financial information, to try to detect early signs of any problems.”*

Of course, prevention is better than cure. Potential customers will be considering a lengthy commitment to a business-critical relationship, and it would be prudent for them to seek detailed information about the financial status (eg: audited accounts, management accounts, shareholder details, insurance cover, etc) of their preferred provider(s) before entering into a contract.<sup>18</sup>

It would be prudent for potential customers to seek detailed information about the financial status of their vendor before entering into a contract.

A vendor may ask the customer to sign an appropriate non-disclosure agreement before releasing commercially sensitive details, but this is perhaps understandable in a new, competitive market. However, customers will probably draw their own conclusions if a vendor appears reluctant to divulge detailed information about its financial position, either initially or at some later stage during the delivery of a project.

... customers will probably draw their own conclusions if a vendor appears reluctant to divulge detailed information about its financial position.

Should transfer of data become necessary, the vendor could offer consultancy services for which the customer may be charged additional fees. Customers should specify that any transferred records are delivered in an industry standard format (eg: XML).

#### Additional contingency

Customers should not accept vendor claims that ‘it will never happen’. BIW’s risk-averse approach includes contingency arrangements that provide for continuity of service regardless of BIW’s status.

Following an agreement with its managed hosting provider Attenda, should BIW cease to be able to trade or continue operations, the BIW service will continue to be delivered for a minimum period of two months at no extra charge. This contingency arrangement is designed to allow sufficient time for former BIW customers to agree a longer term arrangement with Attenda, to agree terms with an alternative hosting service provider, or to run the service themselves on their own server(s) (see *Escrow below*).

<sup>18</sup> The IT Construction Best Practice programme’s *Guidance Note on Project Collaborative Extranets for Construction* (2002) says: “the selection process should include an assessment of the technical, organisational and financial standing of the vendor organisation as the day to day provider of a central service” (p.3) and “system selection should include an assessment of each individual’s financial standing and prospects” (p.5).

## Escrow arrangements

Birkby and Nugent also urge prospective customers to consider safeguards to ensure they can still access the extranet and the information it holds:

*“If use of the extranet or the records it generates requires any proprietary software, then it will be necessary to obtain the source code for this (which most software providers will resist) or to provide for the code to be placed with a third-party escrow agent under an agreement that provides for it to be made available in the event that the software provider or ASP becomes insolvent.”*

### NCC escrow arrangement

To provide further reassurance to its customers, BIW has an escrow agreement in place with the National Computing Centre (NCC). This means that a full copy of the source code relating to the most recent release(s) of BIW software is deposited in escrow with NCC.

Interested customers may be a named party to that agreement enabling them to gain access to the source code in the event that BIW ceased operations for any reason. Being a party to the NCC agreement would enable customers to use an alternative hosting company, or to run the software on their own servers.

## For further information

### Useful web resources

British Standards Institute - [www.bsi-global.com](http://www.bsi-global.com)

Building Centre Trust - [www.buildingcentretrust.org](http://www.buildingcentretrust.org)

Construction Industry Computing Association - [www.cica.org.uk](http://www.cica.org.uk)

GS1 UK - [www.gs1uk.org](http://www.gs1uk.org)

IT Construction Forum - [www.itconstructionforum.org.uk](http://www.itconstructionforum.org.uk)

### Publications

Wilkinson, P. (2005) *Construction Collaboration Technologies: The Extranet Evolution* (London: Taylor & Francis), chapter 7.<sup>19</sup>

<sup>19</sup> Paul Wilkinson, author of this white paper, is head of corporate communications at BIW Technologies, and has been called one of the UK's leading analysts on construction collaboration technologies.