IT Audit Report

Clients

ABC Rental
ZZZ Insurance

Audit Sponsor

Xxxxxx (MD)

Document Control

Version	1.0 (Draft)
Author	Robin Bennett MA (Oxon) FIAP MIoD, Start Services (Director)
Contact	robin.bennett@start-services.co.uk, 07971 696157
Quality Checked by	Kim Evison MA (CantAB), Quality Manager
Date of issue	27 November 2009

Contents

Methodology

This report has been compiled following two short site visits (on 9 & 17 November 2009) and keeping time spent within a limit of two days as specified by the audit sponsor. During the second visit, a teleconference was held with Xxxxxx (BBB Ltd) with Xxxxxx and Xxxxxx present.

This is a report *by exception* showing items of note or concern; where no such items were found, no report is necessarily made (although in some cases it is for clarity). For this reason, the audit may appear to be essentially negative and critical, however this is not intended to be the case and care should be taken when reading the report to keep this in mind.

Each paragraph is uniquely numbered in the margin for reference.

I would like to thank the management team and staff of ABC and ZZZ for their friendly assistance during the site visits and during subsequent telephone enquiries.

Definitions

"Management Team":	Xxxxxx, ABC Rental (Managing Director) Xxxxxx, ABC Rental (Finance Director) Xxxxxx, ZZZ Insurance (Sales Director)
"PC":	Desktop and/or laptop computer running Windows 98, 2000, XP or Vista
"Server":	Server-class computer running Windows Server 2000, 2003 or 2008

Executive Summary

Key Areas of Note or Concern

ES1 New investment is currently being made to replace the old server with a new, more secure setup and better hardware. This will put the businesses on a better footing although arguably some opportunities have been missed at this time (see AR6, AR7).

ES2 Most PCs have a consistent set of office productivity and anti-virus software. Some minor improvements can be made here (see AR14, AR19).

ES3 Other IT/telephony infrastructure is either sound or being upgraded.

ES4 There is a lack of clarity in terms of direction and control of IT issues which is the result of historical changes within the management team and the lack of a specific "IT Manager" post. This is not unusual and is not a major concern, but increased transparency here would be helpful to the businesses moving forwards (see AR1, AR2).

ES5 The key business software – RRR – is functional, well understood and has stood the test of time. However, it is showing its age and a web-based alternative could give the businesses more opportunities in the market. There are plans to develop major upgrades.

ES6 Generally the IT risks and opportunities in the businesses are well understood.

ES7 The key risks (acknowledged by the management team) are around the use of "one-man-band" developer Xxxxxx. The working relationship has been productive and has suited both parties, but there is some confusion and lack of agreement as to the ownership ("IPR") of the software he writes and supports, despite a written agreement being in place from February 2006. There is also the issue of cost and whether his service represents value for money (see AR28, AR29, AR32).

ES8 With the exception of the issues described in ES7, the businesses are moving forwards in an appropriate direction. ES7 is the key risk and needs to be properly addressed.

ES9 The remote server contract appears to be significantly over-priced and has an unusually long "lock-in" period (see AR39, AR40, AR41, AR42).

Key Recommendations

ES10 Revisit the proposal from SSS to see whether additional resilience/redundancy can be built into the new server setup at minimal cost (see AR7).

ES11 Reassert the nature of the relationship with Xxxxxx and set an appropriate level of fees (see AR21, AR25, AR32).

ES12 Revisit the contract for the remotely-hosted server to see if renegotiation is feasible (see AR39, AR40).

Management Structure

AR1 There is no-one specifically with the job title "IT Manager" or "IT Director" in post. Xxxxxx said that he was now responsible for IT within ZZZ following a transfer of responsibility from Xxxxxx. Xxxxxx also assists with the IT for ABC, though Xxxxxx leads here (with Xxxxxx heading up retail IT).

AR2 With the added complication of the two inter-related companies, there needs to be absolute clarity in terms of who is ultimately responsible for all matters IT.

PCs

Hardware

AR3 All PCs should have at least 1GB of RAM in order to be suitably productive. At the site visit, one PC, Xxxxxx's, had only 512MB and should be upgraded.

Operating Systems

AR4 Most PCs have a variation of Windows XP and there is consistency throughout. Some PCs are at Service Pack 2 level (SP2) and others are at SP3. This is not going to cause you an immediate problem but suggests an inherent lack of control and application of Windows Updates. You should review policies and procedures here.

AR5 One PC, Xxxxxx's again, has XP Home rather than XP Professional. XP Home cannot connect to network domains and so this will need to be addressed before you switch over to the new server. I was assured that this was in hand.

Server(s)

AR6 The server is in the process of being upgraded per the proposal from SSS Ltd.

AR7 The proposal itself is sensible and Xxxxxx appeared to be competent and in control of the system migration. However, the result of the spend will be another single-server system (albeit a more secure and easily managed one); with this level of investment it would be natural to assume that a step-change in resilience would have been the end-result.

Telephony

AR8 The current system is doing its job adequately. There are opportunities to take advantage of new technologies (eg VoIP) when the next system upgrade is planned.

Security

Physical

AR9 Appropriate protection for the server is in place.

AR10 Concern has been expressed about security in general at the offices. For this reason, I would recommend additional security for desktops and, in particular, laptops used in the front offices. Laptops can be easily and cheaply secured to desktops using "Kensington security cables."

Backups

AR11 I was assured that appropriate onsite and offsite backups are in place. In addition to keeping backups, regular "trial restorations" should be actioned to ensure that the backups are actually working.

Disaster Recovery

AR12 We discussed the disaster recovery options at the meetings. If the disaster recovery arrangements are not documented, they need to be and copies distributed throughout the management team.

Anti-virus

AR13 Panda anti-virus was present and has been automatically updated on all PCs bar one. The other PC had Kaspersky anti-virus.

AR14 The ideal situation is for a company to have a mix of anti-virus products on site (as no one product protects against all known malware). For this reason, I would recommend that you consider additional/alternative products when Panda becomes due for renewal.

Passwords

AR15 At the moment, there is no consistent use of passwords and no associated password policy.

AR16 When the new "domain" is instigated, passwords will be enforced as part of a domain policy. User training will be needed to explain the new policies and procedures relating to domain passwords (and other domain-related issues) at this time.

Standard Desktop Software

Licensing

AR17 I was informed that Microsoft Office is licensed properly throughout the organisation.

AR18 You should consider less expensive forms of licensing when it is time to upgrade. The next release of Office, Microsoft Office 2010, is due shortly and may well be priced much more competitively as alternatives (such as Google Docs and Open Office) are either free ("open source"), paid for by advertising or simply much less expensive.

Consistency

AR19 Most PCs have Office 2007 installed although a small number still have Office 97 (eg Xxxxxx's and Xxxxxx's). Free "Compatibility Packs" are available for download from Microsoft which can enable PCs to access documents created using the latest versions of Office but these are a poor substitute for the full version of the software.

AR20 When Office 2010 is released, it is worth reconsidering the standard level of software deployed, taking into account upgrade costs.

Bespoke Software

Supplier Status

AR21 Xxxxxx is a "one-man-band" software developer. This is not uncommon in the industry and his daily rate (£nnn) is towards the top-end of the range of sole trader developers.

AR22 RRR – the bespoke software in question – is in use at ABC and ZZZ and is also installed and used by franchisees (ABC) and licensees (ZZZ). Xxxxxx is paid a fee for each copy installed to ABC and ZZZ customers.

AR23 He has been writing software in this market for 15+ years (10-12 with ABC) and has a good understanding of requirements and a long-standing relationship with the management team.

AR24 ABC and ZZZ are now Xxxxxx's only major clients and this means that the product direction is defined largely by the management team and not by Xxxxxx himself.

AR25 Concerns were expressed at Xxxxxx's ability to deliver changes in a quality manner. Recent changes (such as the VAT change to 15%) took a number of attempts to get right.

AR26 Xxxxxx is using Delphi to develop the software. The product is a little "old fashioned" in appearance although is tidy and the user interface looked consistent.

AR27 Xxxxxx has informed me that Key Man Insurance is in place. This policy and the level at which it pays out should be regularly reviewed.

Ownership/Intellectual Property Rights (IPR)

AR28 The management team (Xxxxxx, in particular) had expressed a view that ABC owned the copyright to the software and that paperwork existed to back up this assertion. A copy of this written agreement (dated 20 February 2006) has been forwarded to me by email.

AR29 In contrast, Xxxxxx expressed the opposite view during our teleconference. His claim was evidenced by explaining that he had originally written the software (approximately 15 years previously) for an entirely different client before starting to work for ABC/ZZZ.

AR30 Xxxxxx's belief that he owns the rights to the software is also supported by the practice of paying him a licence fee ("royalty payment") for each copy sold.

AR31 The written agreement looks sound but confusion clearly remains.

AR32 This issue needs to be resolved quickly but without upsetting the current relationship that exists. This whole aspect is the most significant IT-related business risk that I have found during the audit.

AR33 Both parties confirmed that copies of the source code are deposited at ABC after major changes have been made although this process appears to be somewhat ad-hoc. This procedure should be formalised and records kept of each deposit made.

Remotely-hosted Server

AR34 A remotely-hosted server and application is used to score insurance requests.

AR35 The server hosting agreement between TTT Limited and ABC Limited was given to me for comment.

AR36 ZZZ are included in the contract because they are a connected or group company, ie have the same or substantially the same shareholders as ABC.

AR37 The agreement is dated 1 June 2009 and specifically mentions an initial 5-year contract period.

AR38 It is a "reasonable endeavours" contract which is fairly typical in format. It has a target of 99% uptime. This again is fairly typical though at the lower end (99.5% or 99.9% is more usual).

AR39 The hosting fee is £nnnn per annum. Market rates for server hosting have dropped dramatically over the last 3 years and a typical price for 99.9% uptime is now between £nn/month and £nnn/month depending on server specification. Unless TTT is also recovering software fees (and there is no mention of this in the contract) it is difficult to justify this level of expense which is between n and n times the typical rate.

AR40 Cancellation on either side is possible but *not within the first 5 years of the agreement.* This is very unusual. Typical server hosting contracts run for an initial period (6 or 12 months) with a subsequent 3-month notice period.

AR41 The daily rates for staff as shown in the Additional Services list ("Schedule 1") are expensive.

AR42 Unless there is good reason for the charges to be higher than typical or for the length of contract being longer than normal to which I am not party, this contract does not appear to be in the best interests of ABC.

Internet

Email

AR43 Email is hosted externally and is deemed to work satisfactorily.

Policies

AR44 I was told that users have been told (via written memo) what constitutes acceptable use of the Internet at work. I have not yet seen a copy of this document.

AR45 If employee files do not contain a signed copy of this memo (acknowledging that it has been read and understood) then this situation needs to be addressed.

Web Sites

AR46 The two related web sites shown to me are www.ABCxxx.co.uk and www.ZZZinsurance.co.uk .

AR47 An analysis of content, design and search engine positioning was outside the scope of this audit.

Domain Names

AR48 *ABCxxx.co.uk* is a valuable domain name and special care needs to be taken to ensure continued ownership (single word domain names are typically worth £n on the open market). It is up for renewal on nn December 2009. It is correctly registered to "ABC Ltd".

AR49 *ZZZinsurance.co.uk* is also registered to "ABC Ltd". Should this properly be registered to ZZZ? This has a renewal date of nn January 2011.