IT Audit Report

Client

XXX Group

www.XXX-group.com

Audit Sponsors

XXX (Administration Manager)

XXX (Chief Executive)

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	2 March 2010

Contents

Focus of Audit

Start Services was asked to prepare an IT audit of XXX Group's systems and capabilities focusing on the ongoing concerns and dissatisfaction with IT expressed by the users across the company (UK and beyond).

Methodology

This report has been compiled following two half-day site visits (on 22 & 23 February 2010) and keeping time spent within a limit of two days as specified by the audit sponsors.

During the second visit, telephone calls were made to satellite offices as follows:

- XXX from the XXX office
- XXX from XXX
- XXX from XXX
- XXX from XXX.

During the site visits and subsequently, a number of documents have been emailed to me by XXX, IT Manager, and these have been very useful in compiling a complete picture of the IT situation.

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 XXX and XXX for their friendly assistance during the site visits and during subsequent telephone enquiries.

Executive Summary

Key Areas of Note or Concern

ES1 All users spoken to expressed dissatisfaction with the IT systems currently in place. The level of concern varied from mild irritation with "niggles" through to grave concern that the perceived poor reliability of the current setup prevented business from being done in a timely manner.

ES2 Inevitably, the competence, aptitude and attitude of XXX, the IT Manager, was an area of discussion. I'm pleased to report that all users expressed their belief that XXX was capable and personable. However, most also said that he appeared to be "overworked" and that he did not communicate his activities well enough. This is also the opinion that I drew during my discussions with him.

ES3 The previous IT support individual (XXX) continues to be involved peripherally but he is less than helpful to XXX on occasions and his lack of urgency when invoicing for services or hardware supplied means that a figure approaching £100K is being "carried over" in the books. This arrangement needs to be resolved and put on a professional footing or else brought to a close.

ES4 XXX has to balance proactive "project" work with reactive "helpdesk" issues and he currently has no reliable method for assessing and communicating priorities.

ES5 XXX has recently assumed responsibility for IT and has started to improve how XXX is being supervised. There is more to do here although a good start has been made.

ES6 XXX has no system or method in place to log issues raised by users and so each office has invented a different mechanism. A single company-wide solution should be implemented to resolve this as soon as possible.

ES7 The current server setup is comprehensive although possibly over-complex. In addition, there is little sharing of roles across the installed servers so the system is vulnerable to downtime as it has many single points of failure. This can be addressed by making better use of the servers already installed.

ES8 A recent move to install a server in XXX with a replicated copy of the Profile database has not gone smoothly. Although some issues will always arise, this may be suggestive of a lack of planning. It is not clear yet whether the XXX server will resolve the issues being seen.

ES9 There is currently no formal disaster recovery plan in place and so business continuity is vulnerable and threatened by fire or other significant event.

ES10 The current Citrix-based "thin client" environment has many benefits to the organisation centrally (eg ease of administration, security, software distribution and upgrading) but it almost inevitably gives the users a less-than-perfect experience and one which compares poorly with their experience of home and directly-connected work PCs.

Key Recommendations

ES11 Install a company-wide issue tracking "system" immediately and ensure that there is complete visibility of XXX's workload throughout the organisation (see AR12, AR13).

ES12 Either put the relationship with XXX on a formal, professional footing or else bring it to a close (see ES3, AR23, AR30, AR66).

ES13 Give XXX some support either by recruiting a part-time support/helpdesk technician for employment internally, or by contracting with a support company (preferably with a local base) to provide occasional cover for when XXX is not available (see AR5, AR6, AR7, AR8).

ES14 Ask XXX to review the server roles so that there is an increased level of redundancy (see AR18, AR19, AR21).

ES15 As a management team, review the decision to log user activity at such a detailed and invasive level (see AR37, AR38).

ES16 Across the business, develop a disaster recovery plan (of which IT will form a major part) and review/update it regularly (see AR44, AR45, AR46).

ES17 Ask XXX to review the pros and cons of the Citrix environment and present his findings to the Board and other key stakeholders in the business (see AR22 ,AR40, AR55).

IT Management/Structure

AR1 There is a clear management structure in place with XXX in post as IT Manager, supervised by XXX, Administration Manager. XXX reports to XXX, Chief Executive.

AR2 XXX is suitably remunerated and has been in post for nearly two years. Until recently, he reported to the part-time Financial Director.

AR3 XXX has recently been moved into the main office from Accounts. This has enabled him to feel more "part of the team" and was a very good move. I suggest that the link with XXX is strengthened by moving XXX across to sit next to XXX if possible.

AR4 XXX's background and 16 years of varied IT experience are the right ones for the post he currently holds. Ongoing professional development is always important in a technical role and XXX should actively pursue training opportunities during her formal 12-monthly employment reviews with him.

AR5 XXX feels somewhat isolated in his role, a common situation where only a single individual works to support the IT for a business.

AR6 A consequence of being isolated in the role is that he has not felt able to "bounce" ideas of others or to adequately find alternative solutions to problems as they arise. A good example would be the time it took to switch back to BT from Global Crossing for International calls when Global Crossing appeared to be unreliable.

AR7 Another consequence of being the sole IT support for the business is that he is rarely if ever "off duty" and often takes calls at weekends or when on holiday. This is not an ideal situation.

AR8 If XXX had some internal assistance (a part-time IT support technician) or external help from a capable IT support business, he would be able to discuss projects and problems with others and this would help him to prioritise issues and resolve them more quickly and to the users' satisfaction.

AR9 XXX has implemented frequent planning meetings (weekly/fortnightly) and these will also help.

AR10 During our meetings, XXX impressed with his maturity, self-awareness and open attitude. These attributes are not typical of IT managers and technical staff.

AR11 XXX's time management, prioritisation and organisation skills are not well developed and need to be improved. Support from XXX allied with formal training should improve matters.

AR12 All users spoken to expressed positive feelings towards XXX – they essentially like him – but all feel that he does not communicate well enough with them. The comment "when we get him on the 'phone he is fine" was common – but without a system for logging problems, lower priority issues are bound to get lost.

AR13 XXX needs to implement a system for logging, prioritising and reporting problems as a matter of urgency. This could be a shared Google Docs (see http://docs.google.com) spreadsheet, for example, or a more comprehensive package incorporating problem management, inventory and

monitoring such as Spiceworks (see http://www.spiceworks.com). Spiceworks is well-used and well-liked and has the not inconsiderable advantage of being free!

AR14 Finally, as IT Manager XXX is able technically to access emails for all employees. Although this is normal, it is usual for an IT Manager's contract to state that the reading of emails sent to others should only be done with the express permission of his/her line manager – this is to protect him/her as much as it is to protect the other employees. I suggest you implement such a change to his contract.

Client Devices

Desktop

AR15 Most users operate their systems via Wyse Winterm thin-client units. Some users have access to the system through laptops or desktop PCs.

Mobile

AR16 Blackberry handhelds running Internet Blackberry are in use across the company with no concerns being expressed about their use or performance.

Servers and Datacentre

AR17 There are 14 servers active in the business providing a variety of services including Citrix function, Profile, domain control and Exchange (email).

AR18 All servers are currently physical boxes and the relatively new, powerful and efficient virtualising techniques have not been explored within the company. This is an oversight and something which XXX should address.

AR19 In the current setup, the mail service (for example) is vulnerable as only one server is configured to provide Exchange and so a hardware failure in this server would cause downtime to the business while the server was rebuilt. This downtime could easily stretch to a few days. Again, XXX needs to look at this area of business.

AR20 The Sybase database supporting Profile is also vulnerable to hardware failure (although slightly less so now that the replication server has been shipped to XXX).

AR21 The volume of data being stored within Exchange as a whole and by individual users is growing to the point that an archiving solution will become necessary very soon. XXX needs to investigate and report options to XXX.

AR22 The Citrix servers are well configured in a farm of 4 devices with auto load-balancing.

AR23 The server data centre is in the process of being moved from XXX to XXX (XXX) as part of the decoupling from XXX and this is a sensible move.

AR24 There is a SQL Server database containing the data for the old Red Rabbit system. This is interrogated only when necessary.

AR25 A network attached storage (NAS) box is also present though currently non-functional.

Network

AR26 The XXX office is connected to the Datacentre via a 2Mb leased line.

AR27 All other offices are connected to the Internet via standard business broadband.

AR28 This is an arrangement typical of your size of business.

AR29 XXX has supplied diagnostic data showing network speed between locations and all is satisfactory.

AR30 The Draytek routers on each site cannot be interrogated because XXX will not release the access user ID and password to XXX as he says it would "compromise the security of his other customers". As reported, this is nonsense and the access codes for the routers should be given to XXX as a matter of urgency.

Telephony

AR31 Now that international calls are being routed via BT, the telephone system is deemed to be reliable enough again.

AR32 The telephone maintenance arrangement is sensible and value-for-money at approximately £XXX per year.

AR33 I was told that you had entered a 5-year deal with Global Crossing for telephone services. This length of contract is longer than typical for telecommunications contracts and in a fast-moving sector it is unlikely to give you the best price or the best service over the contract period.

AR34 The hacking of the system last year with the subsequent £XXX bill has not been resolved completely and should be put to bed with lessons learned.

Security

User Monitoring

AR35 Spector 360 from SpectorSoft (see http://www.spectorsoft.com) is used to monitor the activities of all users at an extremely detailed level.

AR36 Although security is key in your industry with the constant threat that employees either leave and take confidential data with them or will pass/sell data to competitors, this level of logging is unusual.

AR37 Although well-regarded and apparently reliable, logging software of this type must inevitably have an impact on the performance of the servers. As the software has hooks into the operating system at a very low level, it is also likely to be the cause of some of the "random" glitches that users experience.

AR38 I recommend that you reflect on the decision to log activity at such a low level as a management team and implement a less invasive alternative if you decide that this is more proportionate.

Physical

AR39 With the majority of servers being housed at the datacentre, they are no more or less secure than the datacentre. I did not visit the datacentre and so cannot comment.

AR40 Thin-client computing is inherently secure as the Winterms are not as desirable to thieves and there is no data stored on them.

AR41 XXX should reflect on the security of laptops and data stored on them.

Backups

AR42 Appropriate server backups are in place.

AR43 On advice, XXX has changed some of the incremental backup operations to differential (which are larger in size but much quicker to restore in the event of a system failure).

Disaster Recovery

AR44 There is no formal disaster recovery plan for the business. IT forms a major part of a disaster recovery plan, but all departments and functions need to be fully engaged in such a plan.

AR45 A good disaster recovery plan will cover situations such as fire or flooding to major locations, alternative working arrangements should a main building be out of action, recovery from theft of servers or server data, and the process to be followed in the event of a major fraud or data theft/corruption within the business.

AR46 I strongly recommend that you prepare your plan as a matter of urgency.

Documentation

AR47 At regular intervals, checks should be made to ensure that all system passwords (eg SQL server “sa” passwords) are recorded and accessible to staff other than XXX in the event of an emergency.

Anti-virus

AR48 Sophos is used through the organisation and is automatically updated.

AR49 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 Sophos becomes due for renewal.

Passwords

A consistent and sensible password policy is in force as a part of the domain management policies.

Standard Desktop Software

Office

AR50 Microsoft Office is the office productivity suite of choice.

AR51 As the worldwide standard, this is a normal and sensible choice though many organisations are looking to switch to open source or cloud-based alternatives to save money or to increase productivity and flexibility of working.

Internet Browsing

AR52 Internet Explorer 7 is in use throughout. I suggest you try Chrome as a faster alternative especially as the slow performance of Internet Explorer is a key concern for users.

Licensing

AR53 I was informed that Microsoft Office is licensed properly throughout the organisation.

AR54 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

AR55 With the software being provided via the Citrix environment, consistency of software versions is guaranteed and is a major benefit of this style of operation.

Industry-Specific Software

AR56 Microdec Profile (www.microdec-profile.com) is used as the company's software of choice for managing the process of finding and placing candidates.

AR57 Profile is a well-regarded and well-used piece of software in the recruitment industry.

AR58 Users throughout XXX expressed general satisfaction with Profile although some areas were identified as being areas of concern including the email integration facility which was less user-friendly and capable than "straight Outlook".

Other Software

AR59 Accounts use Exchequer (on CITRIXC) and expressed no concerns at all with the software.

AR60 The bank dial-up system has now been replicated to a second PC in the Accounts Office and so this single point-of-failure has been resolved.

Internet

Email

AR61 Email facilities are provided by Exchange and generally work well though the integration with Profile was often criticised by users.

AR62 As previously mentioned, the Exchange Store is growing very quickly and so an archiving solution should be investigated and trialled.

Policies

AR63 Excellent staff policies are in place which state the limits of personal use of the Internet. The policies are well-worded and very mature in attitude.

Web Sites

AR64 The group's main website is to be found at http://www.XXX-group.com/ with subsidiary sites at http://www.XXX-XXX.com/, http://www.XXX-XXX.com/ and http://www.XXX-XXX.com/.

AR65 An analysis of content, design and search engine positioning was outside the scope of this audit.

Domain Names

AR66 XXX still controls the administration of some of the domain names and XXX is moving domains to be under XXX's direct control as and when they become due for renewal. Consideration should be given to a more proactive approach to this process.