WITN00740120

POLB(11)32

POST OFFICE LTD BOARD

POL IT Audit Update (SAS70)

1. Purpose

The purpose of this paper is to provide an update on:

1.1 The progress against the Ernst & Young IT & Change focused audit recommendations
1.2 The current status of the review of adopting SAS70

2. Background

2.1 There were ten key recommendations from the audit which were classified as 4 high, 3 medium and 3 low.
2.2 The recommendations related to change management processes; access controls; the Fujitsu managed service and POL's oversight of key control processes within Fujitsu.
2.3 The audit over ran this year against Ernst & Young's planned timescales, with additional costs to POL amounting to £135k.

- POL were not engaged in setting the timescale, there was no recognition from the previous audit or indeed the complexity of the changes to the systems during the year and the assumption by Ernst & Young was that the audit would not highlight any control weaknesses and hence no retest.
- POL and Fujitsu have undertaken significant changes to the financial systems environment this past year. The entire counter and branch support systems (consisting over 30000+ counters and 12000+ branches) converted from the Horizon system to Horizon next generation (HNGX).
- Secondly the Post Office financial systems consolidated from many systems into one. This also included the supporting change management processes and systems within Fujitsu to support POL's customer requirements.
- This resulted in an additional level of complexity as both old and new systems required auditing. Additionally, the Ernst & Young team were new to the account and had no understanding of the POL systems which required a steep learning curve.
- These contributed to the cost overrun. Early engagement with Ernst & Young will remove that risk this year.

3. Progress update

Since the audit we have made good progress on all the actions and remain on track to complete these by the end of October.

3.1 An Audit Steering Group has been established for IT related audits which have now met on three occasions. This provides the appropriate level of governance and oversight to ensure that the audit actions are completed as agreed and the alignment of all our compliance audit requirements.
3.2 We have engaged with Ernst & Young since the 2010/11 audit concluded to build relationships, share progress and plan for this year's audit.

WITN00740120

3.3 A project team has been established within Fujitsu to manage all activities which are currently on target for completion by end of October:

- Fujitsu have completed two of the recommendations, namely strengthening the change management process and improving the problem & incident management process.
- One of the high findings was in respect of the level of oversight and assurance of control processes within Fujitsu. We are working with Fujitsu to build a reporting process to ensure visibility of Fujitsu's control environment is transparent to POL through regular reporting activity.
- Five of the recommendations relate to user management and access rights to POL's systems. A complete review of this area is underway and is on target for completion.
- There are 3 independent actions being progressed within POL which are well underway and we expect will be completed ahead of the end of October. These refer to improved user management controls within the Post Office finance system for cash services, a review of the testing process for maintenance / BAU changes (to ensure that a consistent approach exists and is followed, with regular audit to monitor compliance) and the creation of a central store of approvals for go-live decisions given to Fujitsu.

3.4 Group Risk & Audit and Fujitsu are to undertake an independent review of the completed actions during October and November to provide assurance that all actions have been satisfactorily completed. The key review findings will also be fed into the ongoing action updates with Ernst & Young to provide assurance of completion.

3.5 In summary, all recommendations from the Ernst & Young audit are being actioned and in some cases are complete. They are all on track for completion by the October target date. In addition, we have taken on a number of lessons learnt from the last audit to improve the way of working with regard to the audit and are working closely with Ernst & Young and our suppliers to put these improvements in place ahead of this year's audit.

4. Assessing the need for a SAS70 audit approach

4.1 SAS70 (Statement on Auditing Standards No. 70) is a recognized auditing standard developed by the American Institute of Certified Public Accountants (AICPA) for American based companies. It reports on the controls within a service organisation. It is currently being replaced in the US by SSAE16 and by ISAE3402 which is the international standard. The effective date of the introduction of SSAE16 was 15 June 2011. If implemented in the UK it is likely we would adopt the ISAE3402 approach for non US based organisations, but for the benefit of the remainder of this paper we will refer to it as SAS70.

4.2 It is a requirement for any company listed on the Wall Street stock exchange to adopt the SAS70 standard. Each company has to be audited annually and to fail an audit could result in the removal from those indices.

4.3 The Ernst & Young audit management letter recommended that POL should keep SAS70 as an option and under consideration as a framework for its service management controls.

5. Decision to adopt SAS70

5.1 We are in discussion with a number of companies beyond Fujitsu that use SAS70 to get a better understanding of the benefits that may exist for POL and the steps necessary to implement a this audit approach. These include Ernst & Young, Deloitte and CSC.

WITN00740120

5.2 In addition, we are currently in discussions with Fujitsu regarding the future of their current service contract, which is subject to a separate paper provided to the Board (Fujitsu Horizon online contract renewal in 2015).

5.3 We intend to further investigate the standard and include it as part of the commercial discussions with Fujitsu and as part of the audit for 2012/13.

5.4 As part of the strategic approach and the introduction of a supplier framework, we will also ensure that SAS70 is a key requirement.

5.5 Introduction of SAS70 will have a positive impact with regard to our clients and key stakeholders who will recognise the controls our service providers have over our key financial systems, similar to PCI compliance currently in place for the Payment Card Industry.

6. Migration implications

6.1 A SAS70 annual audit and the output report, which is produced by an accredited auditor for the service industry, can cost the service provider in excess of £300k to produce and this is based on an engagement of circa nine months for the audit including any pre work to define scoping, internal testing to be assured of compliance, the actual audit and the report writing.

6.2 If Fujitsu undertook SAS70 then the output report from the audit could then be made available to POL and then can be shared with our auditors or clients, which would provide evidence that our suppliers systems and controls are robust with regard to the financial transactions. It is likely that this arrangement would make the POL IT controls audit a more efficient process.

6.3 Fujitsu currently undergo a number of external audits against compliance including ISO27001 for Security, ISO20000 for Service Management, ISO 9000 for Quality, LINK DSS for our LINK accreditation, PCI for our compliance with the Payment Card Industry, Ernst & Young for the IT Controls to support the financial audit and a variety of other external audits, internal audits or RM Group audits determined each year.

6.4 To assist in this audit complexity Fujitsu are developing an audit framework, where each set of requirements for the multiple standards are captured into a framework system that identifies the evidence once required for a number of standards. We are investigating if the current Ernst & Young general IT controls could be adopted into this approach alongside PCI, ISO, LINK etc. Additionally SAS70 standards could also be captured in this tool.

6.5 We understand from liaising with Gartner, CSC and Deloitte that an organisation would require between 8 to 12 months to develop the internal controls and processes to align with a formal SAS70 audit requirements.

6.6 Currently within the contract we require Fujitsu to meet a number of standards e.g. ISO standards 27001 for security, ISO9564 for PIN Pads but not SAS70. A change to the current contract and commercials would be necessary to adopt SAS70 and the impact of this is still under review.

6.7 It is believed that this standard has not been developed with the concept of shared services and cloud architecture as there are no established audit principals that can be directly applied; the impact of this on the applicability of the standard to POL will be reviewed.

7. 2011/12 audit approach

7.1 As discussed in section 3, in response to the audit recommendations made by Ernst & Young we will have enhanced service management controls in place by the end of October which will be independently audited by both Group Risk & Audit and Fujitsu.

7.2 A comprehensive 2011/12 audit plan is being developed to ensure that:

- Ernst & Young are assured of completion of actions relating to the audit recommendations;

WITN00740120

- They are consulted on and in agreement with our approach for the adoption of SAS70 by the end of 2012 for the 2012/13 audit;
- That those impacted (POL and Fujitsu) by the 2011/12 audit are fully briefed on the requirements of them, the meeting schedules, evidence and documentation required.

7.3 Audit kick-off is scheduled for 20th September; walkthroughs / interviews planned for October and November; follow-ups planned for January and February.

8. Summary

8.1 In summary, we will have enhanced controls, governance and a reporting mechanism in place with Fujitsu, covering the recommendations made by Ernst & Young, by the end of October, with an intention to move to SAS70 by the end of 2012 for use as part of the 12/13 audit.

9. Recommendations

The POL Board is asked to:

9.1 Note the progress against the actions raised through the Ernst & Young audit management letter and that the end date for completion remains on target.

9.2 Note the work currently underway with regard to investigating the potential adoption of SAS70.

Mike Young
Chief Operating Officer
September 2011