FUJ00086922

Briefing note on Audit findings for Senior Management

Executive Summary

Given the scope of the audit and the significant changes to the key financial systems being investigated, the findings from the 2010/11 audit are significantly focussed.

POL and Fujitsu have undertaken significant changes to the financial systems environment this past year. The entire counter and branch support environment (consisting over 30000+ counters and 12000+ branches) converted from the Horizon system to Horizon next generation (HNGX) along with the consolidation of the SAP back-office environment into POLSAP, and the provision of supporting change management processes and systems within Fujitsu to support POL's customer requirements.

The new HNGX environment is now a full production environment and Fujitsu is in the final stages of transitioning all supporting environments as part of this progression from a major development.

There are 3 main categories to be addressed,

- the Change Management Process and it's controls,
- User Access and appropriate authorisations and
- the extent to which POL require proof of management activities from the Fujitsu Managed Service.

Ernst & Young have identified 4x High priority, 3x Medium priority and 3x Low priority findings.

The complexity of the POL/Fujitsu environments has required a more technical understanding from the auditors vs previous years, and the utilisation of the shared service approach (ie the utilisation of a shared, secure List X data centre shared with other customers including Government) has introduced further complexity and difficulty in gaining audit evidence. The utilisation of these shared services have contributed towards the £50m savings to POL for IT services.

The hours utilised this year doubles that of last year's audit – but given the scope of changes applied and the total revisit of the evidential information request, this is not unexpected.

Audit interaction

Ernst & Young auditors have been provided with significant support from all parties involved with the audit, and certain key personnel have been identified for recognition. Due to the significant system changes this audit period, the original information requests had to be totally reworked which created additional workload within POL and Fujitsu.

In spite of the markedly changed environments, new information requests and the necessity to explain the changes to the financial systems as well as the supporting change management systems, the audit completed more than 5 weeks earlier than last year's audit.

Financials

Ernst & Young have stated that an over-run against Plan has occurred.
However, neither POL nor Fujitsu were engaged in the production of the Plan, and

- no prior years engagements were factored in, (2010 overrun doubled the Plan estimate)
- the significant impact that the changes of POL FS to POLSAP and Horizon to HNGX made to
    - the original evidence requests,
    - re-engineering request to the new environments or
    - gaining evidence from remarkably differing financial systems.
- Insufficient time allocated for a new team reaching an understanding of the new environments

The estimated budget for Ernst & Young to complete this year's review, based on the assumption that evidence would be readily available and that all controls would be in place was 457 hours. Actual time spent from E&Y was 1195 hours which included a figure of 75

FUJ00086922

hours for internal E&Y overruns due to a new team being engaged with no experience of the POL estate, which is extremely conservative.

Contractuals

The Post Office and Fujitsu operate 180 Operational Level Agreements against the contractual obligations for the Managed Service incorporating HNGX and POLSAP financial environment.

These operational level reviews are primarily focussed on the business-facing services and do not necessarily cover the support systems that Fujitsu operates behind the scenes to manage the environments from development to production through all its stages.

However, a Security Managed Service: Service Description does exist that '*provides a range of security-related activities that support the establishment and maintenance of an ISO27001 compliant infrastructure. The Security Management Service monitors operations and introduces specific protective security controls to maintain the integrity, availability and confidentiality of information used and produced* '

This includes ongoing assurance of security policies and procedures, reviews of operational processes, monthly plans to address audit and compliance issues and monthly reporting on existing service changes, among other activities.

Recommendations

It has been recommended that activities take place in certain key areas to resolve applicable audit findings

1. POL/Fujitsu contract to clearly state expectations and ensure monitoring of requirements to support control activities is in place to support controls identified
2. Fujitsu to resolve certain access control issues around financial systems
    a. Resolution of user or system accounts that create segregation of duties conflicts
    b. Ensure processes are in place to ensure regular review of access controls and cleanup of access rights due to personnel changes
3. Fujitsu continue to improve change management processes
    a. ensure visibility to POL of process controls
    b. ensure adequate traceability of approvals

While certain mitigating controls are in place through Fujitsu's global best practices there are opportunities to improve specific controls, visibility of controls and mitigating processes and POL's management interactions to continue to assure the environment.

FUJ00086922

Appendix A – Audit Findings

Ernst & Young have generated 10 key findings

Finding	Priority	Summary	Responsibility
1	High	The governance of the outsourced environment is complex and difficult to gain control evidence	**POL** – review contract to identify control management requirements **Fujitsu** – ensure visibility, end-to-end process
2	High	Segregation of duties within the controlling of the manage change process to be confirmed	**POL** – ensure controls are managed **Fujitsu** – balance best practice and segregation of duties
3	High	Strengthen the change management process regarding approvals required	**POL** – ensure clear evidence of approvals process **Fujitsu** – balance best practise with need for fixes
4	High	Review of privileged access for administration and technical resources	**POL** – ensure controls are managed **Fujitsu** – ensure appropriate access, control on regular schedule
5	Medium	Implement periodic user access reviews and monitoring controls	**POL** – ensure controls are managed **Fujitsu** – implement regularly scheduled access control reviews
6	Medium	Strengthen the User Administration Process	**POL** – ensure controls are managed **Fujitsu** – review user access process with full traceability
7	Low	Improvements to logical security settings for administrators	**POL** – ensure controls are managed **Fujitsu** – balance best practice and segregation of duties
8	Low	Strengthen the password parameters	**POL** – ensure controls are managed **Fujitsu** – balance best practice and system capabilities
9	Medium	Review of generic privileged accounts	**POL** – ensure controls are managed **Fujitsu** – balance best practice and segregation of duties
10	Low	Improvements to the problem and incident management process	**POL** – ensure controls are managed **Fujitsu** – ensure best practice followed