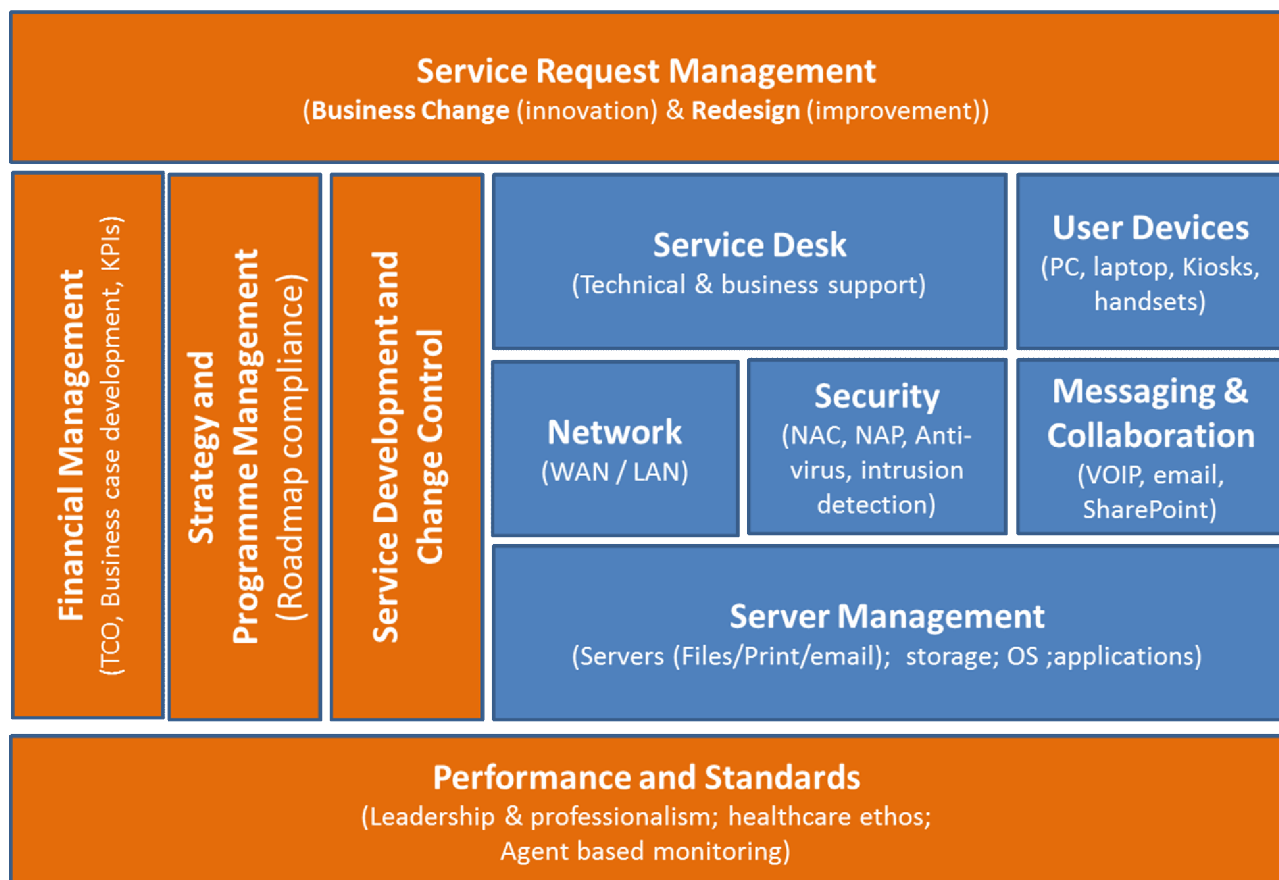


**REGULAR REPORT:
SSA ICT DIRECTORATE
OCTOBER 2010 TO DECEMBER 2010**

Introduction

The Directorate has undergone a change of leadership and re-alignment to the key organisation objectives of the PCT and has worked very much more closely with colleagues from Information Governance. It is important that the focus on Information Security and the close working relationship between Information Technology and Information Governance is retained and built upon. The leadership of both teams are determined to ensure that this happens. The model below is part of this process and shows the strategic architecture that overarches both the working relationship between the teams and the target structure for the future – some of the model is already in place, other elements will be worked on over the next few months.

- Governance function
- Infrastructure function



GOVERNANCE FUNCTIONS

FINANCIAL MANAGEMENT

The Directorate is forecast to break even at the end of the Financial Year and focus on cost management and reduction is being maintained. A number of maintenance contracts for servers and software are due for renewal before the end of March each of these will be evaluated for any further cost reductions and to ensure that they are cost effective.

The business case for the improvements in the information security infrastructure has been created and is close to final approval. A programme plan for the work to implement the business case is being worked on.

A member of the Server Management Team resigned in December and finished 10th January 2011, a number (4) of Fixed Term roles will finish at the end of March 2011 and other Fixed Term role will expire in June and July. In total 12 staff are currently on Fixed Term contracts – 2 of which for the Trainers in Health Team will expire in 2012.

A framework agreement for the provision of IT staff from external agencies was sent for approval in December – this agreement is the result of a process undertaken by the Healthcare Purchasing Consortium.

PERFORMANCE & STANDARDS

An Operational Stability Plan was created in December with a new management approach for the Directorate including a daily operational review process. The operational review process has been in place for more than a month and is now entrenched in the daily working of the Directorate and has been expanded to include colleagues from other departments.

The Directorate has fully supported the remedial work required as a result of the Serious Untoward Incident reported by a failure of the information security systems that are the responsibility of the Directorate. Members of the Directorate have been involved in several security review activities:

- Security Report performed by Jo Watts, ICT Security Manager, Wolverhampton PCT,
- internal Root Cause Analysis activity carried out by Alison Braham
- Audit by the Information Commissioner's Office.

Lessons have already been learned as a result of the incident and the investigations listed above; work is on-going to ensure that all agreed actions are carried out and that the culture of the Directorate correctly reflects the importance of Information Security and the responsibility that the Directorate has in this regard.

The Directorate Risks and Issues Log is currently being revised to the same standards as that used by other Departments and Directorates, and will be linked to the Board Assurance Framework.

A number of policies relating to Information Security were identified as missing and a process put in place to allow for the rapid development and authorisation of these policies – this activity is on-going.

The Directorate has 4 key work areas going forward, in order of priority:

1. Operational Stability
2. ITIL & Governance

3. Toolkit/Information Security Management Systems (due 31.03.11)
4. Project list – mainly for Birmingham Community Healthcare

Strategy & Programme Management

The Information Security SUI had a major impact on the planned programme work of work for the reporting period. The majority of the programme plan was halted, the only exceptions being those projects that directly supported the transition of PCT staff to BCHC. Key activities for this function now underway are the development of an overall IT strategy, an Operational Stability Plan and the Information Security Business case. The Information Security Business Case will generate a significant amount of work for the Directorate as various new systems are deployed and changes made to existing systems.

SERVICE DEVELOPMENT & CHANGE CONTROL

A review of the Change Control Board has commenced with a view to expanding the brief of the Board, membership, strategy and the governance framework for the Board. The Trainers in Health team continue to expand use of the system across the country and recently submitted a report to the House of Lords. The Directorate supported the transition of Community Service staff to BCHC through the change of users to a new e-mail address, Intranet homepage and screen saver. Follow-up activities to move user data are now under discussion. The application staff development teams developed software to support the work of the Trust in creating the Information Asset Register. A large scale architecture model of the IT infrastructure across Birmingham was created and made available to Trust Directors – work to build on this model will continue in the months ahead.

SERVICE REQUEST MANAGEMENT

The work of the Project Office was severely impacted by the diversion of technical resources to the SUI however some small scale projects for BCHC were able to continue. The team also rolled-out the upgrade to the ESR system required for the start of the New Year.

All the technical infrastructure teams were impacted by the response required to the SUI and the audit by the ICO. The User Devices team had responsibility for dealing with the folder permissions issue and creating a much more secure folder structure, they also produced a detailed report showing all permissions. The Server Team had responsibility for the file archive work that was carried out. The Network Team reviewed the current state of the network security especially with regard to the wireless network. All three teams contributed to overall response to the SUI, the Root Cause Analysis and the audits.

Each of the teams are now working on developing a strategy for their area which will form part of the overall IT strategy for the infrastructure and applications supported by the Directorate.

INFRASTRUCTURE FUNCTIONS

SERVICE DESK

The Service Desk changed direction during the reporting period to have a much greater focus on call response times and abandoned calls. New systems and processes are in place to support the change in direction. The call volumes for the reporting period are down which may well indicate that this new approach is helping to reduce overall call volumes.

October 2010 = 4253 (25% decrease)
October 2009 = 5612

November 2010 = 4415 (17% decrease)
November 2009 = 5319

December 2010 = 3322 (24% decrease)
December 2009 = 4344

Obviously other factors may also be part of this reduction e.g. the snow and ice, reduction in staff numbers, improvements to systems.

USER DEVICES

The devices team have played a large role in the response to the Information Security SUI and have focussed their efforts on resolving folder permissions as raised by users and performing a rapid review of the permissions existing at the time of the incident and working with colleagues across the Trusts to review those permissions and amend them in line with instructions received.

NETWORK

No major outages were reported during the period.

SECURITY

No major anti-virus outbreaks took place in the reporting period – continual monitoring of virus threats is carried and reported on a daily basis. Over the 3 month period the average daily infection rate for all users is 0.16% or about 9 reported per day.

MESSAGING & COLLABORATION

E-mail services have operated normally during the reporting period. Some delays with e-mails were reported and have been investigated. Our investigation revealed that the delay was within the Connecting for Health relay systems that process e-mails from the outside world and forward them on to our local Exchange servers.

SERVER MANAGEMENT

As part of the housekeeping activity initiated by BENPCT to support the creation of the Information Asset Register an archive activity on the file & print servers was undertaken which moved all files which had not been modified in the past 18 months to a “data vault” – no data was lost as a result of this activity but a 60% reduction in the “live” files held on the main server was achieved. It has been suggested that a similar activity is undertaken by the other Trusts supported by the Directorate.