Business Process Improvement: Mr Roy Dunn

1. Human resources

There are no changes to BPI structure.

2. Quality Management System (QMS) review meetings, internal audits and Near Miss Reports (NMR).

The internal audit schedule for 2013 – 14 is running.

Two further NMR's (non-conformance incidents) have been declared. A summary report of all Near Miss Reports will be presented at this next Audit Committee. One report has been completed.

3. QMS process updates

A review of the UK Registrations process is about to begin. There are likely to be some changes to the tendering & procurement processes over the next few months. Council member recruitment process and Independent prescribing have been drafted.

4. BSI audit

BSI Audited the Policy, Registrations UK applications and employee training, HR and Partners areas on 7th October 2013. No areas of non conformance were found. The report will go to this Audit Committee.

The HCPC QMS / ISMS will be migrated to the new BSI platform as soon as possible.

5. Business continuity

A final paper only version of the Business Continuity plan has been circulated. Monthly details will continue.

6. Information security management

We have modified the security training CBT package for all employees, with the Secretariat department. User details have been supplied to the supplier and will be in use by end of the month.

Partners and Members will be trained on information security using the CBT package used by employees last year. User details have been supplied to the training company.

Adjustments to how documents are printed around the organisation are being evaluated, and security improvements developed. The IT department have seen two possible providers of technology solutions.

A clear desk policy (at least no personal information) is being developed for the organisation. This will form part of the organisations Information Security Management System (ISMS).

The new ISO 27001:2013 standard are more significant than initially indicated. EMT decided on the 19th November to go straight for the new standard, as the duration of the old standard is a maximum of 18 months.

UKAS have yet to accredit a certification body and BSI have not yet audited to ISO27001:2013. Changes to the Information Security standards to which we wish to certify have several impacts on the requirements for us to achieve the required standard of compliance.

The new ISO 27001 standard does not formally invoke the Plan-Do-Check-Act (PDCA) methodology. However, Annex SL does state the following:

"An effective management system is usually based on managing the organization's processes using a Plan-Do-Check-Act approach in order to achieve the intended outcomes."

All of the new standards are replacing the "PDCA approach" with a "risk management approach", which initially seems less onerous. However more detailed on going monitoring of risks, at a granular level is required.

The number of sections in Annex A has changed from 11 to 14. The number of controls across all sections has changed from 133 to 114.

The order of the controls has changed and all recorded risks mitigated by those controls must be remapped. This is a somewhat arduous task, that the BPI department will attempt on behalf of the rest of the organisation. We then plan to certify against the new standard ISO27001:2013 from scratch, rather than certify against the old standard, and migrate to the new. Overall this will decrease the effort required, but will make a slight delay to the certification date.

Work on developing a secure web delivery method for confidential content for various parts of the organization continues, with an existing supplier.

7. Information & data management

Assessment and destruction of older archive material: an update on progress.

We have destroyed 248 boxes of old material so far, including registration files from the 1960s into the 1970s, and boxes containing old finance material from the 1990s and early 2000s up to the seven year retention period required for financial material. There has therefore been a reduction in the number of boxes in the archive for the first time since we began recording numbers. In the immediate future we propose to destroy all the Registration Department's application and renewal boxes up to January 2006, namely over 1,300, as all applications from the start of CPSM through to HPC have either been microfilmed or scanned. We will then discuss with Registrations how we deal with their remaining boxes, from 2006 to the present.

We will also be discussing with the Communications and Fitness to Practise Departments their individual requirements.

Freedom of Information requests of a statistical nature continue.

8. Reporting

Some changes to how security is implemented around the Crystal Reports database, have required changes to existing reports. Those of an operational nature are being addressed first.

9. Risk Register

The last Risk Register was presented to Audit Committee in September. The next iteration will be published in February 2014.

The ISO definition of Risk across all standards has been defined as;
“*The effect of uncertainty on objectives*”

10. Other activity

The tendering process for the security print contract commenced and the PQQ has been published.