Business Process Improvement: Mr Roy Dunn

1. Human resources

The Quality Compliance Auditor (Kayleigh Birtwistle) has undertaken the BSI ISO27001:2013 Internal Auditor course, along with 11 other colleagues from around the organisation.

This will assist in our ongoing requirement to audit across the business, and have local expertise on interpreting the Information Security standard.

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

The internal audit schedule for 2015 – 16 is running.
The access rights of all employees and contractors will be evaluated over the coming months, and we will be looking for updates to Education department processes as their new IT system beds in.

NMR’s

One new NMR was opened and has been completed since March.

3. QMS process updates

The migration of the Quality Management System (QMS) to an externally hosted system has been terminated. The new access model following an upgrade to the hosting platform was found to be incompatible with our click through access requirement. We will therefore be planning to migrate our QMS & ISMS to a hosted MS SharePoint environment over the autumn.

4. BSI audit

The ISO9001:2008 audit took place on the 29th & 30th April.
Overview: Quality Management System Processes, Communications and Fitness to Practise were audited.

An Observation was raised concerning the determination of what could be defined as undue delay in making changes to systems.

A copy of the report is provided in a later paper.

5. Business continuity

An upgrade to an externally hosted Business Continuity System will be made when legal sign off of the contract has been achieved. The hosting site is ISO27001 certified.

6. Information security management

Various Information Security awareness activities have taken place around HCPC. These include; Infographics, competitions, team briefings, intranet posts and news stories. These were designed to ensure employees were fully aware of the requirements to achieve ISO27001 certification.

ISO27001 certification is a two stage process. Stage 1 assessment is a general look at the organisation,

Company Overview – Organisation Context, Interested Parties and Scope Leadership / Compliance
Management System, Policies and Objectives, Documented Information Organisational Planning and Control,
Tour Facility
Senior Management (if possible)
Risk Assessment – General Information Security Risk Assessment
Information Security Risk Treatment and Statement of Applicability
Resources, Competence, Training and Awareness Communication
Monitoring, measurement, analysis and evaluation Internal Audit and Management Review Non Conformity and Corrective Action and Improvement
Closing Meeting: Discuss readiness for Stage 2

The Stage 1 ISO27001:2013 assessment by BSI took place on the 31st March. Two auditors attended for one day. Considerable examination of the documentation around our alignment to the 27001 standard was examined. A tour of the campus also took place.

There were two Observations;

1. A small amount of packing material in the server room holding a component.
2. There was no evidence that residual high level risks had been specifically signed off by the EMT.

There was one Opportunity for Improvement, around removal of personal waste bins next to desks, in favour of communal bins in central departmental locations

There was one Minor Nonconformity around listing those responsible for delivering objectives, and those responsible for reporting on objectives not being split out in the documentation.

The report recommended that we were ready to go forward to the Stage 2 assessment.

The Stage 2 assessment took place on 20 -22nd May with two auditors on site for 1 ½ days, one auditor for the remaining days. (4 ½ days of audit in total)

Opening meeting: administration, business and ISMS change
Top Management: leadership and commitment, context of the organisation, objectives and targets, and ISMS performance improvement
Review previous report, confirm status of ISMS and scope
Context of the organisation: internal/external issues and interested parties
Legislation and compliance
Risk management, and statement of applicability
Access Control & Cryptography
Operations Security
Communications Security
System acquisition, development and maintenance
Supplier relationships
Physical & Environmental security
HR

Finance Team (security awareness sampling)
Project Management Team (security awareness sampling)
Communications Team (security awareness sampling)
Policy & Standards (security awareness sampling)
Fitness to Practise (security awareness sampling)
Registrations (security awareness sampling)

Information security awareness sampling was carried out across the organisation, plus audit of specific processes.

Two Observations were raised;

1. The cabling at the back of one network cabinet was seen to be untidy. This remedial work is planned for when the server room is expanded, and a new rack can be purchased.
2. Maintenance records for the air conditioner units in the server room were not immediately available. (These were located on the following day).

Two minor nonconformances were raised.

The previous nonconformity from the Stage 1 assessment had been resolved satisfactorily, but had not been recorded in the improvement log.

The Tidy Desk Policy was found not to be adhered to as some PC's were found without locked screens.

HCPC were recommended for certification. The next Continuing Assessment Visit is due for April 13-14th 2016

7. Information & data management
Assessment and destruction of older archive material: an update on progress.

The Registration department hope to progress the destruction of scanned renewal notices as soon as the archive boxes can be validated as “renewals”. A pre destruction visit to the archive is being planned.

Work with the Registrations department on sites for secure scanning continues prior to tests with internal CPD processes.

8. Reporting

The number of Freedom of Information requests of a statistical nature has slowed.

9. Risk Register

The last iteration was published in March 2015 following updates over the winter. The next iteration will be based on updates collected over June-August this year, with publication due for September.