Finance and Resources Committee – 17 March 2011

Business Process Improvement Work Plan 2011 - 2012

Executive summary and recommendations

Introduction

The attached document is the proposed Business Process Improvement work plan for 2011 – 2012. It details the key objectives, the main areas of work and what we intend to develop within the Business Process Improvement area over the next financial year.

Decision

The Committee is asked to agree the attached Business Process Improvement work plan.

Background information

This document is intended to supplement the Council's strategic intent document and sits alongside other departmental level strategy and work plan documents such as Communications, Finance, IT, Projects, Education, Policy & Standards, Human Resources, Registrations and Fitness to Practise.

It is a working document and is therefore always under review.

Resource implications

See attached work plan.

Financial implications

See attached work plan.

Appendices

Business Process Improvement Work Plan 2011 – 2012.

Date of paper

4th March 2011

BUSINESS PROCESS IMPROVEMENT Work plan 2011-12

Roy Dunn – Head of Business Process Improvement

Operations Directorate

Introduction

Business Process Improvement maintains develops and promotes the Quality Management System, Information Security, Risk Analysis and information reporting services used by HPC. Management Reporting is carried out, as are ad-hoc reporting and data extraction for the business. Business Continuity and process improvement are also developed and maintained. Equality & Diversity processes are monitored within Quality audits. Business Process Improvement reports to the Audit and Finance & Resources Committee.

The department also now delivers the 5 year rolling registrant forecast, based on parameters supplied by internal and external sources.

This document

This document has been drafted to set out work priorities for the financial year April 2011 – March 2012, and to provide a basis against which the work of the Business Process Improvement function can be planned and measured.

Resources

The Business Process Improvement consists of 2 full time employees, plus additional support:

Name	Role	ISO standards
Roy Dunn	Head of Business Process Improvement	9001; 27001
Tom Berrie	Information Services Manager	9001
Cherise Evans	PA to Director of Ops (part-time, additional support to BPI)	9001

Future resourcing.

All those listed above are trained to carry out internal ISO 9001 audits. As we have operational responsibilities, and audit responsibilities it is essential that we do not have to audit our own work. (For example Cherise Evans does not audit the customer service function)

As ISO27001 is adopted, we will need to ensure this practice continues, to maintain validity of the management control systems. As Roy Dunn is building the information security function in HPC, it is imperative that an additional person is trained as an internal ISO27001 auditor before the BSI gap analysis is carried out..

Tasks and Projects completed in 2010-11

1) ISO9001:2000 Maintenance and raising the profile of Quality Migration to 9001:2008 [Risks 2.3, 9.1 Quality Management]

The ISO9001: 2008 standard to which we have been certified, has been externally tested, with audits by BSI in June and November 2010, and our certification is retained.

Business Process Improvement average an internal audit every month over 2010-11. through a combination of Departmental audits, risk based audits and across company audits. Supplier audits have also been carried out, namely ServicePoint, a scanning, copying and printing contractor (two sites) and Deepstore, an archiving contractor. An audit of our new prime print supplier is due for January/February 2011

All new staff are given induction training which includes the reasons for use of ISO9001 at HPC.

More robust Corrective and Preventive action processes have been implemented.

2) Improvement to Quality Management System software [Risks 2.3, 9.1, Unacceptable service standards, maintenance of ISO registration]

The HPC Quality Management System (QMS) was created using Microsoft Front Page. The software was no longer sufficient for purpose, and was upgraded to use Lotus Notes functionality as planned. Further controls were required resulting in the development of document and record control functionality, that supports the ongoing maintenance of our registration under ISO9001 & future standards.

A list of processes can be output from the system for use in internal and external audits. Versioning is automatically controlled on process pages. These changes are recorded in a log. A Feedback form has been added and has attracted 3 inputs to the system to date.

3) ISO27001 & BS25999 standards + PCI DSS Compliance – Credit card industry [Risks 2.1, 5.3, 15.7, 17.1, 17.2, 17.3, 17.4; Data Security]

The creation of an ISO27001 Information Security Management System (ISMS) and BS25999 Business Continuity Management system (BCMS) combined with our existing Quality Management System were postponed due to cutbacks in discretionary spend at HPC. Some low level policy work and training has continued on ISO27001. The HPC Information Security Policy was signed off by EMT in September 2010.

4) Selection and purchase of enhanced statistical reporting tools [Risks 2.3, 9.1, Unacceptable service standards, maintenance of ISO registration]

HPC currently use a combination of Excel, Crystal Reports and DBVisulizer to extract and report on trends in data.

A high volume of custom reports have been created around CPD, Online register emulation, various snapshot checks of registration data before and after the running of NetRegulate batch processes.

A more sophisticated tool is required to enable more robust analysis using standard statistical techniques. This includes Root Cause Analysis, a requirement for maintaining ISO9001:2000/2008 under 8.2.1, 8.4 and 8.5.1

The Minitab tool has been installed on a single laptop, but minor issues flagged by the software as licence problems have delayed use to date. (HPC does have a full user licence.) It may be beneficial to install this software on a traditional PC at some stage in the future.

Tests are on going.

5) Disaster Recovery / Business Continuity – ongoing development, testing and training [Risks 2.1, 2.5, Business Continuity]

HPC have used 3 days of testing at ICM in the 2010-11 financial year. Members of the EMT & CDT business continuity teams were taken to Uxbridge and taken through a detailed scenario with continually changing information.

Services were restored by the IT team from the Uxbridge site, linking to the Reading / Rackspace data centre where our replicated data is held in a warm environment.

A report on the test was delivered to the Finance and Resources committee.

6) vsRISK in support of the ISO27001 project [Risks 2.1, 5.3, 15.7, 17.1, 17.2, 17.3, 17.4; Data Security] (item added after submission of initial plan)

A software system was purchased to track the information assets used by HPC. This is an essential requirement of the ISO27001 standard. Threats and vulnerabilities and mitigations / controls must be tracked long term by HPC to achieve and maintain this standard.

This tools key output is the statement of applicability, a unique deliverable in the ISO27001 project that must be revisited at least every year. Population of the tool has commenced.

Additional major items undertaken

Business Process Improvement have also been involved in the following;

- CPD Audit with University of Readings Statistical Services Centre.
- Test work on the NHS-electronic Staff Record project.(postponed)
- NHS Counter fraud data extracts
- International application verification project process development
- Additional Risk register work around new professions.
- Data extracts and segmentation for Policy FTP analysis project
- Rolling 5 year registrant and applicant forecasting
- Review of Corrective & Preventive action processes
- Scanning and web presentation project for Registrations CPD assessments and future application online assessment processes.

The level of FOI reporting required by HPC's stakeholders can add a significant burden to the amount of ad hoc reporting required.

2011-12 Activities planned

1) ISO9001:2008 Maintenance and raising the profile of Quality [Risks 2.3, 9.1 Quality Management]

Business Process Improvement aim to undertake an average of one internal audit every month over 2011-12. This will be a combination of Departmental process audits, risk based audits, across company audits and supplier audits. We will of course take into account the variable workloads in other departments and be as flexible as our time constraints allow. Our increasingly robust preventive and corrective action processes will continue to be used as and when required by the organisation.

Information security will be included in all audits in future, and gradually developed to enable all aspects of ISO27001 to be included in the standard **HPC ISO Internal Audit.**

Two external audits by BSI are due to take place in the financial year. This includes a detailed examination of the Quality Management System, International Registrations processes, work environment and infrastructure in April; and Education processes, Secretariat, Purchasing and supply, and Staff development and training in October.

The BPI team will evaluate how our existing **Management Review** processes work, and endeavour to find increasingly robust methods of ensuring all outputs are captured appropriately.

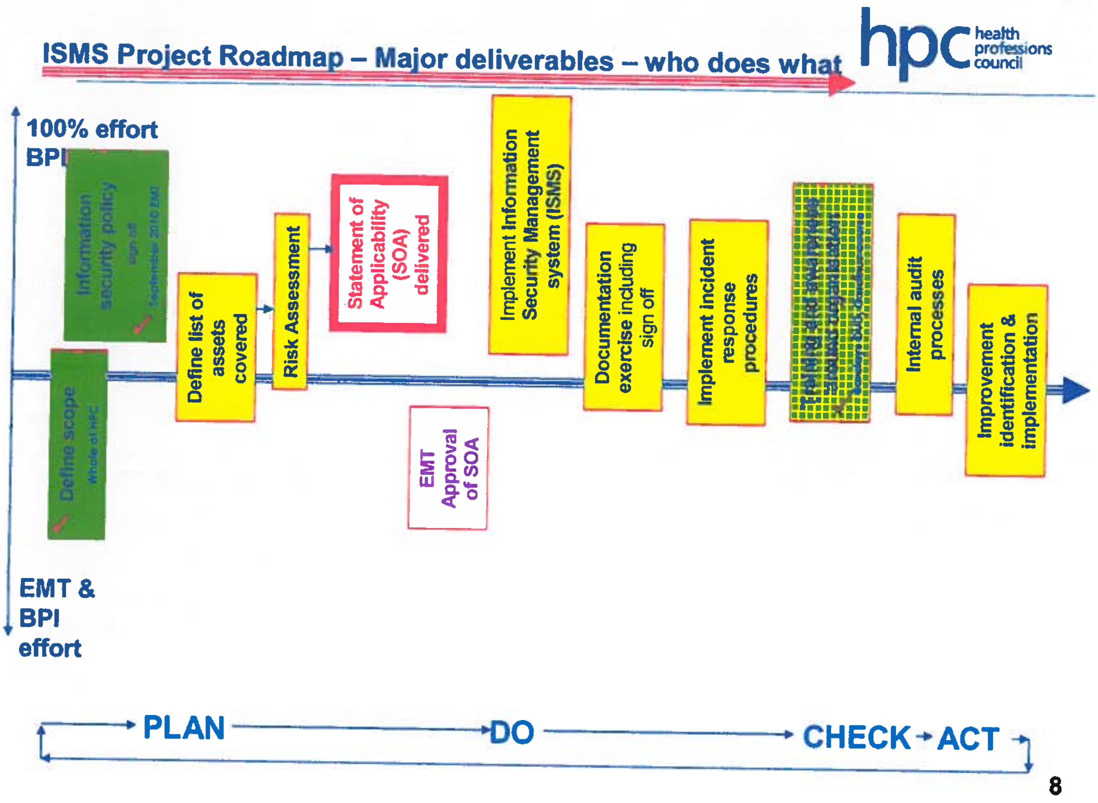
Maintenance of the existing documentation control functionality is required to maintain our ISO9001 registration. Some work may be required to assist the IT department with testing the document control features as the organisation is migrated to Microsoft Office 2010, to ensure it is consistent with the various management systems we operate.

2) Creation of management system and preparation for adoption - ISO27001 (Information Security) standard [Risks 2.1, 5.3, 15.7, 17.1, 17.2, 17.3, 17.4; Data Security]

Following last years work plan publication the discretionary spend on ISO27001 contractor work was abandon in favour of creating a training system for employees. The Cardinus system will be rolled out over December /January 2011. (See **3 Information Security Awareness Employee and contractor training.** below.)

The Information Security policy (a key element of ISO27001) was signed off in September 2010. Work to develop other required documentation and processes will continue without external support. This will thus take longer to achieve, but will enable the Information Security Management System (ISMS) to be more closely matched to HPC's culture and requirements.

The plan for 2011-12 includes the following areas;



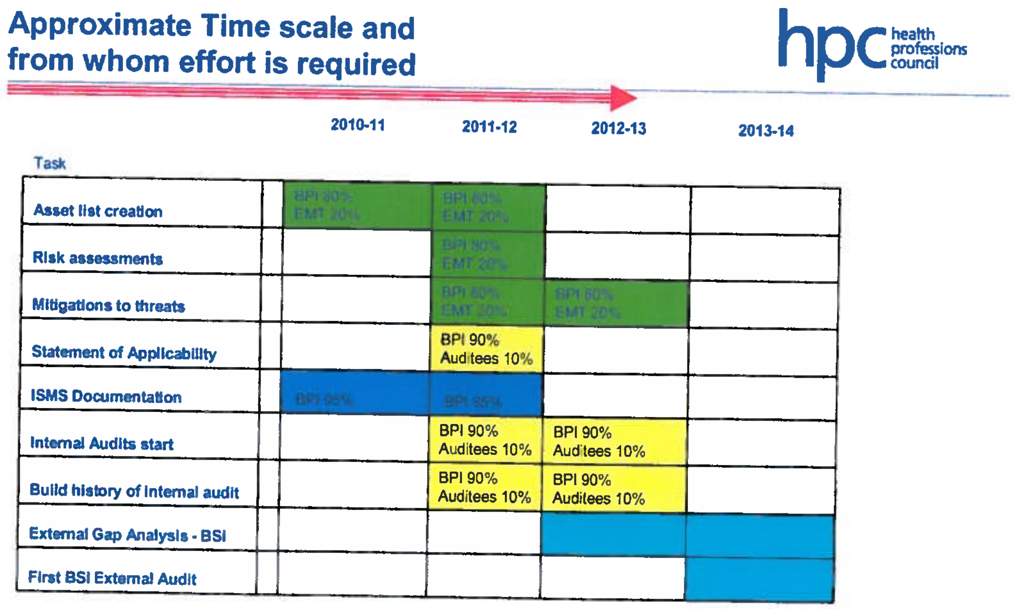
ISMS Project Roadmap – Major deliverables – who does what

hpc health professions council

100% effort BPI
EMT & BPI effort
Information security policy sign off September 2010 EMT
Define scope Whole of HPC
Define list of assets covered
Risk Assessment
Statement of Applicability (SOA) delivered
EMT Approval of SOA
Implement Information Security Management system (ISMS)
Documentation exercise including sign off
Implement incident response procedures
Internal audit processes
Improvement identification & implementation
PLAN
DO
CHECK
ACT

8

The work indicated above sits in the overall plan for ISO27001 as illustrated below;



Approximate Time scale and from whom effort is required

hpc health professions council

Task		2010-11	2011-12	2012-13	2013-14
Asset list creation		BPI 80% EMT 20%	BPI 80% EMT 20%		
Risk assessments			BPI 80% EMT 20%		
Mitigations to threats			BPI 80% EMT 20%	BPI 80% EMT 20%	
Statement of Applicability			BPI 90% Auditees 10%		
ISMS Documentation		BPI 95%	BPI 95%		
Internal Audits start			BPI 90% Auditees 10%	BPI 90% Auditees 10%	
Build history of internal audit			BPI 90% Auditees 10%	BPI 90% Auditees 10%	
External Gap Analysis - BSI				🟦	🟦
First BSI External Audit					🟦

7

BPI aim to map processes and record our adherence to Information Security standards. Monitoring HPC's compliance against the credit card industry standards will continue via process audit and monitoring for changes in the PCI standard.

A separate project on PCI-DSS is in the Finance Departments remit. All PCI-DSS remit data will be re-engineered to be outside HPC.

3) Information Security Awareness Employee and contractor training. [Risks 2.1, 5.3, 15.7, 17.1, 17.2, 17.3, 17.4; Data Security]

Information Security requires ongoing validated training for all employees and contractors, induction training and specialised training for those involved in implementation or auditing of the standards. The Cardinus system will be in place for existing employees and contractors.

However, on going training is required over the year. Following completion of the Cardinus system course additional straining will be delivered through a combination of external training and in house developed content. The costs of developing new security training content for HPC is likely to be in the order of £10,000

Other internal information security training for ad-hoc and All staff meeting use will be produced internally at very low cost.

4) Business Continuity Exercise 2011
[Risks 2.1, 2.5]

HPC will carry out an annual Disaster Recovery / Business continuity test in May, with a predefined scenario. The three day test slot will culminate in a split of EMT and CDT business continuity team members between two sites, and a test of the coordination between the two.

Additional services will be tested, on top of those tested in the past.

The scenario is around lack of building access.

With the Registrations department we will attempt to divert some DDI based telephone services to the ICM suite to be taken by Registration Advisors, updating the live NetRegulate database at Park House.

5) Review of processes around maintenance and availability of HPC's Disaster Recovery plan [Risks 2.1, 2.5]

HPC's hardcopy DR plan has been in it's current format since December 2008.

Although this provides a good general purpose document, it is not easily updated within the sections, and is hard copy based, which creates its own set of issues.

BPI will evaluate existing and future systems that can deliver hardcopy and online content, and determine if these systems can be used by HPC.

Such systems typically cost £5,000 per year plus implementation costs of up to £10,000 – for information only. (This amount is not required In the 2011-12 budget year)

6) Archive Audit and start of document restoration [Risks 17.2, 17.4; Data Security]

a) Following the move of HPC's paper archive to the mine in Cheshire, a detailed audit will take place following operation for approximately every 12 months. This will require the Information Services Manager to stay in Cheshire for 4 nights.

The output will be a check on the categorisation by departmental owner of the new archive, and a check on internal controls around our documentation.

b) Some of HPC's historic documentation, inherited from the CPSM is undergoing trial restoration and preservation. Assuming success of the trial an ongoing programme will continue over time. There are also a number of registration documents that were contaminated in a flood in the 1980's. These require specialised cleaning or secure destruction

7) Proactive examination of HPC's systems and processes.

In light of the white paper and command paper published recently HPC's work load can be expected to continue to grow. On boarding of new professions and new methods of professional regulation will be developed over the next 1 – 3 years. Transaction volumes and types will grow. Therefore the BPI department will proactively search for potential bottle necks in existing processes, and source potential solutions to possible future issues. These are likely to centre around increasing automation and provision of on-line services, enhancing scalability.

Any project proposals determined from this work will be filtered through the Project Prioritisation process.

8) Departmental training

Additional training to allow us to progress the management of HPC's take up of either of the new standards are as follows. The information security standard mandates regular auditor training.

To successfully run ISO27001 we will need to train an additional internal auditor, on the standard. An ISO27001 Lead Auditor has already been trained.

The costs of appropriate training over the next **two** years are potentially as follows;

- Internal Auditor ISO27001 (two days) £1200 = 1 internal auditor
- Introduction to ISO27001 (one day) £500 = Director of Operations
- Information Risk Management (five days) £2150 Hd of BPI?

The exact timing and sequence of training depends on the timing of the core Information Security Management System development.

Ref #	Description	Risk owner (primary person responsible for assessing and managing the ongoing risk)	Impact before mitigations Feb 2011	Likelihood before mitigations Feb 2011	Risk Score = Impact x Likelihood	Mitigation I	Mitigation II	Mitigation III	RISK score after Mitigation Feb 2011
2.1	Inability to occupy premises or use interior equipment	Facilities Manager	4	2	8	Invoke Disaster Recovery/Business Continuity plan	Commercial combined insurance cover (fire, contents, terrorism etc)	-	Low
2.3	Unacceptable service standards	Director of Operations	5	4	20	ISO 9001 Registration, process maps, well documented procedures & BSI audits	Hire temporary staff to clear service backlogs	Market research surveys to prioritise service offerings	Low
2.5	Public transport disruption leading to inability to use Park House	Facilities Manager & Hd Bus Proc	4	5	20	Contact staff via Disaster Recovery Plan process	Make arrangements for staff to work at home if possible	-	Low
5.3	IT fraud or error	Director of IT	3	3	9	Adequate access control procedures maintained. System audit trails.	Regular, enforced strong password changes.	Regular externally run security tests.	Low
9.1	Loss of ISO 9001:2008 Certification	Director of Operations, Head of Business Improvement	4	3	12	Regular & internal audits	QMS standards applied across HPC	Management buy - in	Low
15.7	Registrant Credit Card record	Finance Director	3	1	3	Daily credit card payment reconciliation's in	Tight procedures to retrieve sensitive paper records from	Compliance with credit card record storage standards.	Low

	fraud/theft					Finance dept - Streamline to Netregulate and bank statements.	archive, rationalise records kept and retain sensitive current year records with security tagging.		
17.1	Electronic data is removed inappropriately by an employee	Director of IT	5	3	15	Employment contract includes Data Protection and Confidentiality Agreement	Adequate access control procedures maintained. System audit trails.	Laptop encryption. Remote access to our infrastructure using a VPN . Documented file encryption procedure	Low
	Links to 5.3								
17.2	Paper record Data Security	Head of Business Improvement	5	3	15	Use of locked document destruction bins in each dept. Use of shredder machines for confidential record destruction in some depts e.g. Finance.	Data Protection agreements signed by the relevant suppliers. Dept files stored onsite in locked cabinets.	Regarding Reg Appln forms processing, employment contract includes Data Protection Agreement	Low
	Links to 15.7								
17.3	Loss of electronic data held by third party suppliers in the delivery of their services	Director of IT	5	3	15	Data Protection/Controller agreements signed by the relevant suppliers. Use of electronic firewalls by suppliers.	Data transfer using file level encryption. Physical transfer of back up tapes using specialist company with locked boxes and sign out procedure.	Remote access to our infrastructure using a VPN. Access to third party infrastructure using agreed secure methods.	Low
17.4	Data received from third parties	Director of Ops, and Director of FTP	5	2	10	Read only, password protected access by a restricted no of FTP employees to electronic KN data.	Registrant payments taken in compliance with Payment Card Industry (PCI) Security standards ie with quarterly PCI testing.	Ensure third party data providers e.g. professional bodies provide the data password protected/encrypted/door to door courier/registered mail/sign in sign out as appropriate.	Low

+++++++