BUSINESS PROCESS IMPROVEMENT Work plan 2012-13

Roy Dunn – Head of Business Process Improvement

Operations Directorate

Introduction

Business Process Improvement (BPI) 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 Registrant Forecast”, based on parameters supplied by internal and external sources. BPI also maintain the “Five Year Plan”.

This document

This document has been drafted to set out work priorities for the financial year April 2012 – March 2013, 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 as available:

Name	Role	ISO standards
Roy Dunn	Head of Business Process Improvement	9001; 27001
Tom Berrie	Information Services Manager	9001; 27001
Ruth cooper	PA to Director of Ops (part-time, additional support to BPI) *to be trained in ISO9001*	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 Ruth Cooper 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 and Tom Berrie has undertaken this basic training in 2011.

2012-13 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 audit every month over 2012-13. This will be a combination of Departmental process audits, risk based audits, across company audits and supplier audits.

As HPC are taking on responsibility for Social Workers in 2012-13, 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, Registrations Grandparenting processes, Communications and Secretariat in Spring 2012, Customer Service, Fitness to Practise, and Finance in autimn.

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.

Upgrade of the existing Microsoft Office 2003 document control functionality is required to ease our adherence to document control requirements. Some work may be required to assist the IT Department with testing the document control features as the organisation is now using Microsoft Office 2010, to ensure it is consistent with the various management systems we operate. The work to automate document control across all Microsoft Office applications at HPC will cost in the order of £5,000. This must be completed to maintain appropriate levels of record and document control, without resorting to manual processes.

Business Process Improvement have also determined that a robust Quality Management IT System is required that can be guaranteed to follow prescribed ISO9001 practises. The proposed solution BSI Entropy is externally hosted, includes prompts to complete tasks, and record information as required by the standard. The IT system is being upgraded over the next year or so to include ISO27001 functionality, which will be an obvious benefit. The outright purchase of the software is £10,200. On going maintenance fees will be required in year 2 onwards.

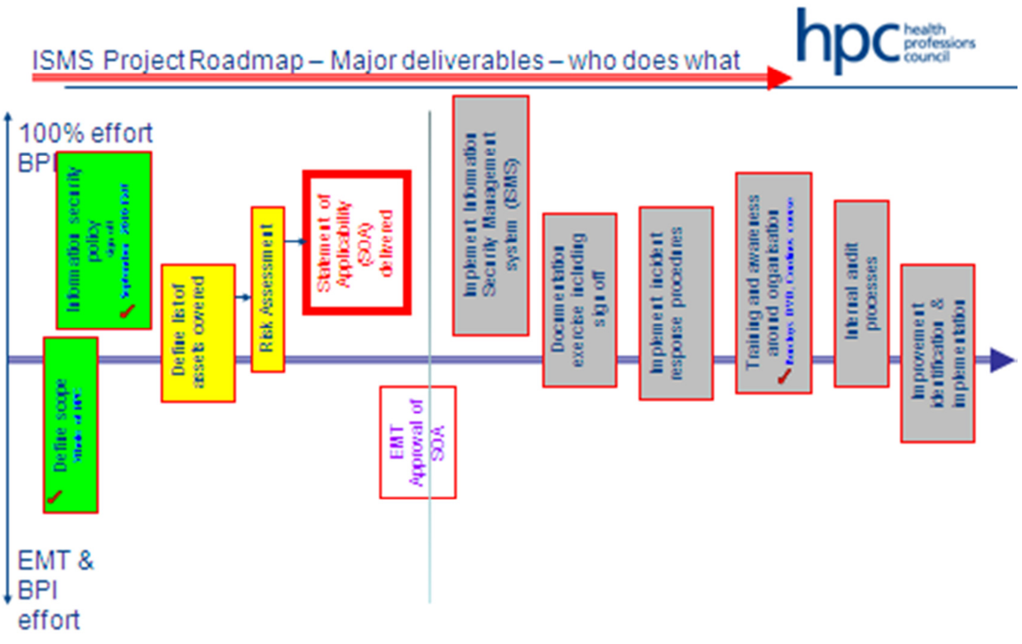
2) Information security management system data gathering exercise for adoption -ISO27001 (Information Security) standard [Risks 2.1, 5.3, 15.7, 17.1, 17.2, 17.3, 17.4; Data Security]

Following last years work plan publication the discretionary spend on ISO27001 was abandon in favour of creating a training system for employees. The Cardinus system was rolled out over December /January 2011. (See **3 Information Security Awareness Employee and contractor training.** below.) and used by all employees. All employees were trained and tested. A new online training solution will be sourced and customised to match HPC's requirements in the 2012-13 financial year.

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 level of information security has been reported as **Substantial Assurance** by Mazars following a risk based audit in Summer 2011
Due to the requirement to adopt the new Project Prioritization process, and to protect critical resources the project has been modified to proceed more slowly, only running up to the creation of an initial statement of applicability. This will progress as far as possible, using internal resources only as they are made available. HPC is undergoing a significant project to take on the regulation of Social Workers in England, and some key systems are completing in the early part of the new financial year. These tasks will retain the highest priority.

The plan for 2012-13 includes the following areas, up to the grey boxes in the diagram below;



ISMS Project Roadmap – Major deliverables – who does what

hpc health professions council
100% effort BPI
EMT & BPI effort
Define scope ✓
Information security policy ✓
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
Training and awareness around organisation ✓
Internal audit processes
Improvement identification & implementation
8

The grey boxes will not be completed in 2012-13 as currently planned.

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 Department's remit. All PCI-DSS remit data will be re-engineered to be outside HPC.

It should be noted that work on increasing security (outside the ISO27001 process) will continue. This includes discrete work within the IT Department, and working with contractors and suppliers.

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 on going 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 has been used for existing employees and contractors. An annual All Employee presentation concerning security and or risk will take place in February, following the current pattern

Futher, on going training is required over the next year. Following completion of the Cardinus system course additional training 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 This will be covering more than basic level security needs.

Again, all employees were trained and tested with a new online training solution to be sourced and customised to match HPC's requirements in the 2012-13 financial year.

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

4) Business Continuity Exercise 2012
[Risks 2.1, 2.5]
HPC will carry out an annual Disaster Recovery / Business continuity test in November/December 2012, 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.

The timing has been arranged to avoid the Social Worker migration project and other major internal projects.

From July to September, the London 2012 Olympics / ParaOlympics are taking place.

Whilst HPC is not directly impacted by the events and venue locations, the travel of employees, partners, Council Members and suppliers could be disrupted or delayed by mass movement of spectators. An additional Risk Register has been constructed, with input from all departments. This will be monitored by the Cross Department Team (CDT) to ensure our resilience over the summer.

Employees are being encouraged to evaluate different travel patterns to ensure they are able to reach the office over the summer.

5) 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. It is desirable to move to a combination of online and paper plans, allowing us to react more effectively to issues that may arise that impact HPC's operations.

A range of technical solutions were viewed at the Business Continuity show in London in November and a demonstration was arranged in house of the preferred solution developed by ICM, our existing business continuity office space provider.

The ICM (Shadow Planner) solution includes triggers to remind those required to input data, to provide the information in a timely manner. The information would be hosted externally, but still produce hardcopy plans for use in house or at EMT & CDT members homes.

An amount has been placed in the Operation projects budget, £25.5k to progress this project.

6) Archive Audit and start of document restoration
[Risks 17.2, 17.4; Data Security]
Following the move of HPC's paper archive to the mine in Cheshire, in 2010 detailed audits will take place following operation for approximately every 12 months. This will require the Information Services Manager to stay in Cheshire for 2 nights. An additional visit to check on basic level security requirements will take place outside the detailed audit.

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.

Historic documentation, inherited from the CPSM continues to undergo restoration and preservation as finance and need arises. The on going programme will continue over time based on need for preservation based on physical condition and importance of the documents. Most of the specialised cleaning has been completed.

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.

This is year two of a two year training cycle to prepare for running ISO27001. The first two sets of training have been completed ;

- Internal Auditor ISO27001 (two days) £1200 = 1 internal auditor
- Introduction to ISO27001 (one day) = Director of Operations, Director of Information Technology and key CDT individuals
- 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 and availability of funds.

9) Modifications to the existing Reporting Tools (Crystal Reports)

The Crystal Reports system will require minor changes to allow new professions to be recognised. Social Worker reporting will be required by July 2012, whilst other new professions will be added approximately 1 month prior to the go live date.

Tasks and Projects completed in 2011-12

1) ISO9001:2008 Maintenance and raising the profile of Quality [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 April and October 2011, with a new BSI auditor and our certification is retained.

A major development of HPC's Projects Prioritisation process has been completed and rolled out, enabling concurrent running of multiple projects at any one of three key stages. Projects can be stopped and started based on business priority.

Business Process Improvement average an internal audit every month over 2011-12 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. Our major printing supplier Europa was also audited.

Work on mapping out Finance Department processes has commenced, with the aim of making processes as robust as possible, prior to taking on new professions. The transactions area has been supported with newly mapped out processes.

This will continue in 2012-13.

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 on going maintenance of our registration under ISO9001 & future standards.

However, the automation of ISO related processes is now dependant on fitting in with other higher profile projects, which may make delivery more difficult. It was determined that moving to a specific ISO9001 compliant system would assist us, and not be subject to internal resource availability. A suitable offering from BSI (our external ISO9001 auditors) has been located and demonstrated. The commercial model for this service has changed since it was last evaluated. It now represents an option for HPC.

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. The PCI-DSS project is due to complete before the end of the 2011-12 financial year, and also includes postal / paper based processes, and the facility for walk in renewal payment via PCI-DSS compliant processes, which were developed with Business Process Improvement input.

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.

The Minitab tool has been installed on a single laptop, but the functionality of Microsoft Office 2010 Excel is being explored to determine what can be achieved with widely available software. Tests are on going.

5) Disaster Recovery / Business Continuity – on-going development, testing and training [Risks 2.1, 2.5, Business Continuity]
HPC have used 3 days of testing at ICM in the 2011-12 financial year. IT team Members were taken to Uxbridge whilst EMT, the Council Chair and other representatives were located in Sevenoaks, Kent and taken through a detailed information loss 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. This will be continued as the ISO27001 project develops.

Additional major items undertaken

Business Process Improvement have also been involved in the following;

- CPD Audit reporting.
- NHS Counter fraud data extracts
- Additional Risk Register work around new professions.

- Data extracts and segmentation for Policy FTP analysis project
- Rolling 5 year registrant and applicant forecasting, involvement with the Centre for Workforce Intelligence modelling process.
- Commence work on development of the Five Year Plan
- Review of Corrective & Preventive action processes
- Scanning and web presentation project for Registrations CPD assessments and future application online assessment processes.
- Additional on going reporting and data extracts to assist Mazars and the Finance Department in resolving the differences between the NetRegulate and Finance Departments deferred income calculations.
- The Risk Management function was audited by Mazars in February 2012. A **Substantial Assurance** grading has been proposed following the audit.
- Olympics – ParaOlympics 2012 Risk Register creation; employee location mapping, supplier accessibility and service mapping.
- Regulating Ethics and Conduct at the CPSM 1960-2002, an historical perspective, by Tom Berrie. Report to be published on the HPC website April / May 2012
- Applications and Registration at CPSM, 1962 to 2002, report by Tom Berrie, first draft for internal circulation.

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

RISKS IMPACTING THE BUSINESS PROCESS IMPROVEMENT AREA

Ref #	Description	Risk owner (primary person responsible for assessing and managing the on-going risk)	Impact before mitigations Jan 2012	Likelihood before mitigations Jan 2012	Risk Score = Impact x Likelihood	Mitigation I	Mitigation II	Mitigation III	RISK score after Mitigation Jan 2012
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 employees 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 employees via Disaster Recovery Plan process	Make arrangements for employees 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 fraud/theft	Finance Director	3	1	**3**	Daily credit card payment reconciliation's in Finance dept - Streamline to	Tight procedures to retrieve sensitive paper records from archive, rationalise records kept and	Compliance with credit card record storage standards.	Low

						NetRegulate and bank statements.	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