Finance & Resources Committee, 18 June 2013

Business Process Improvement work plan 2013-14

Executive summary and recommendations

Introduction

The Business Process Improvement Department is involved in a wide range of activities, and the planned activities are indicated in the attached paper. Progress against last year's plan are also indicated.

The original version of this report was written in April, before the final audit of the BSI ISO9001 cycle had been completed. This audit was passed. We await our confirmation from BSI.

In April, EMT decided to proceed with the ISO27001 Information Security project, with the aim of certifying this financial year, barring major uncontrolled risks being identified. This project is now included in the work plan.

Decision

The Committee is requested to note the document. No decision is required.

Resource implications

Included in departmental plans

Financial implications

Included in departmental budget

Appendices

20130430dQUARPTBPI work plan 2013-14

Date of paper

5 June 2013

BUSINESS PROCESS IMPROVEMENT Work Plan 2013-14

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 HCPC. 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 2013 – March 2014, and to provide a basis against which the work of the Business Process Improvement function can be planned and measured. Activities in this work plan support the delivery of the Business Process Improvement strategy.

Resources

The Business Process Improvement Department consists of 2 full time employees.

Name	Role	ISO standards
Roy Dunn	Head of Business Process Improvement	9001; 27001
Tom Berrie	Information Services Manager	9001; 27001

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.

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 HCPC, it is imperative that an additional person is trained in ISO27001, and Tom Berrie has undertaken this basic training in 2011.

The core skills required for the on going departmental activity are as follows;

ISO9001Lead Auditor Certified x 1
ISO9001 Internal Auditor x1.5
ISO27001 Lead Auditor Certified x 1 (plus currently Lead Implementer)
ISO27001 Internal Auditor x 1
CISMP or other Information Security certification x1
PCIRM or other Information Risk Management certification x 1
Business Continuity Risk Analysis x 1

Business Analysis (ISEB) Certified x1
Requirements Engineering (ISEB) Certified x1
Organisational Context (ISEB) Certified x1

Basic SQL skills (used in ad-hoc report creation) x1
Basic & Intermediate level Excel x 2
Crystal Reports Basic, Intermediate level x1

2013-14 Activities planned

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

The organisation's registration was changed from HPC to HCPC at the time of the November 14th 2012 external BSI audit.

Business Process Improvement aim to undertake an average of one audit every month over 2013-14. This will be a combination of departmental process audits, risk based audits, across company audits and supplier audits. Near Miss Reports may mitigate the requirement for some departmental audits.

Our increasingly robust preventive and corrective action processes, and Near Miss Reporting system 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 **HCPC ISO Internal Audit. This will include the assessment of the departmental assets list, the nature of the threats and vulnerabilities determined, and ensuring the risk scores are appropriate.**

Two external audits by BSI are due to take place in the financial year. This includes a detailed examination of the Quality Management System, which will not have been migrated to the BSI Entropy platform at the time of the audit.

The May audit will include completion of the current three year cycle, the strategic review, and examination of any outstanding issues. Should all of this be satisfactory, the new certificate will be awarded. The next three year external audit plan will be arranged to encompass the entire organisation.

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

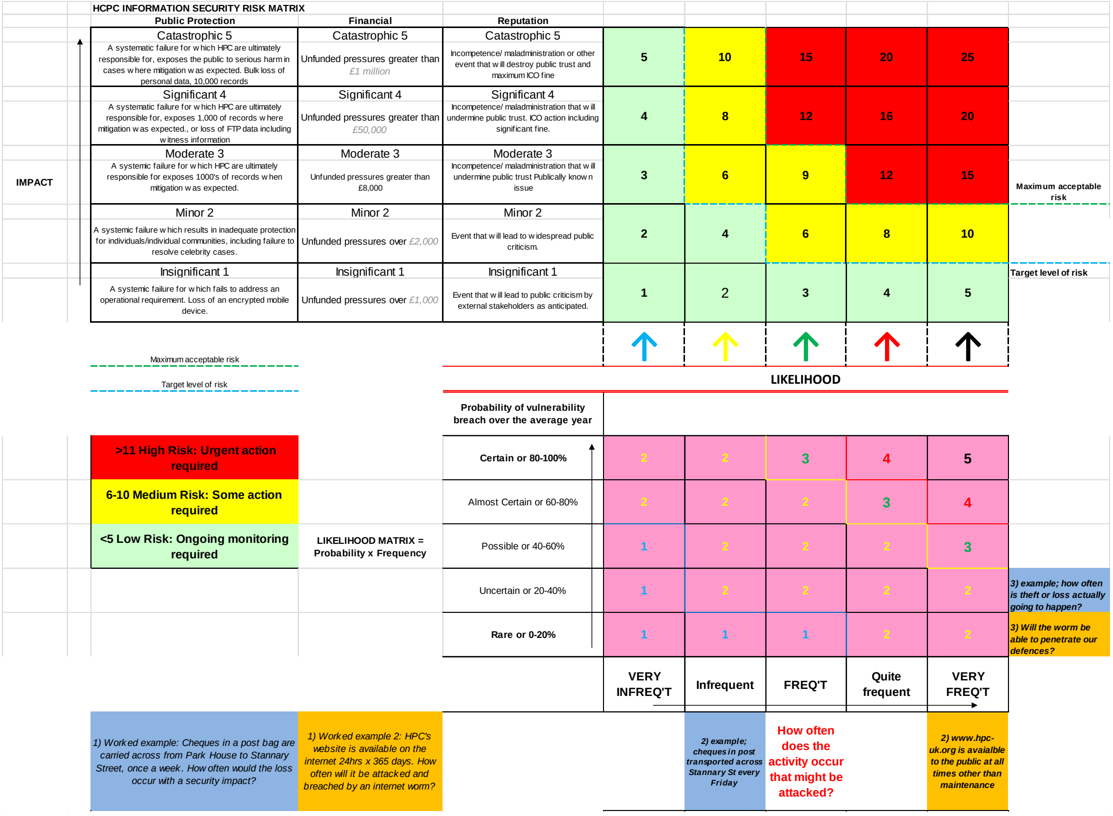
Upgrade of the existing Microsoft Office 2003 document control functionality is required to ease our adherence to document control requirements. Some work may be required to assist the IT Department with testing the document control features as the organisation is now using Microsoft Office 2010, to ensure it is consistent with the various management systems we operate. The work to automate document control across all Microsoft Office applications at HCPC 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.

2) Information security management system data gathering exercise for adoption and preparing for certification stages 1 & 2 -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 IT-Governance system was rolled out over July 2012. (See **3 Information Security Awareness Employee and contractor training.** below.) and used by all employees. This includes specific training around the PCI-DSS credit card standard. All employees were trained and tested. A new online training solution will be sourced and customised to match HCPC's requirements early in the 2013-14 financial year.

The Information Security policy (a key element of ISO27001) was signed off in September 2010. This will now be reviewed in April 2013 and then enter an annual review cycle. Work to develop other required documentation and processes will continue.

The level of information security has been reported as **Substantial Assurance** by Mazars following a risk based audit in Summer 2011. A further assessment was carried out by IT-Governance, in January 2013, suggested an encouraging level of adoption, although more work is still required.



HCPC INFORMATION SECURITY RISK MATRIX

	Public Protection	Financial	Reputation						
	Catastrophic 5 A systematic failure for which HPC are ultimately responsible for, exposes the public to serious harm in cases where mitigation was expected. Bulk loss of personal data, 10,000 records	Catastrophic 5 Unfunded pressures greater than £1 million	Catastrophic 5 Incompetence/ maladministration or other event that will destroy public trust and maximum ICO fine	5	10	15	20	25	
	Significant 4 A systematic failure for which HPC are ultimately responsible for, exposes 1,000 of records where mitigation was expected., or loss of FTP data including witness information	Significant 4 Unfunded pressures greater than £50,000	Significant 4 Incompetence/ maladministration that will undermine public trust. ICO action including significant fine.	4	8	12	16	20	
IMPACT	Moderate 3 A systemic failure for which HPC are ultimately responsible for exposes 1000's of records when mitigation was expected.	Moderate 3 Unfunded pressures greater than £8,000	Moderate 3 Incompetence/ maladministration that will undermine public trust Publically known issue	3	6	9	12	15	Maximum acceptable risk
	Minor 2 A systemic failure which results in inadequate protection for individuals/individual communities, including failure to resolve celebrity cases.	Minor 2 Unfunded pressures over £2,000	Minor 2 Event that will lead to widespread public criticism.	2	4	6	8	10	
	Insignificant 1 A systemic failure for which fails to address an operational requirement. Loss of an encrypted mobile device.	Insignificant 1 Unfunded pressures over £1,000	Insignificant 1 Event that will lead to public criticism by external stakeholders as anticipated.	1	2	3	4	5	Target level of risk

LIKELIHOOD

Maximum acceptable risk

Target level of risk

>11 High Risk: Urgent action required
6-10 Medium Risk: Some action required
<5 Low Risk: Ongoing monitoring required

LIKELIHOOD MATRIX = Probability x Frequency

Probability of vulnerability breach over the average year						
Certain or 80-100%	2	2	3	4	5	
Almost Certain or 60-80%	2	2	2	3	4	
Possible or 40-60%	1	2	2	2	3	
Uncertain or 20-40%	1	2	2	2	2	3) example; how often is theft or loss actually going to happen?
Rare or 0-20%	1	1	1	2	2	3) Will the worm be able to penetrate our defences?
	VERY INFREQ'T	Infrequent	FREQ'T	Quite frequent	VERY FREQ'T	
		2) example; cheques in post transported across Stannary St every Friday	How often does the activity occur that might be attacked?		2) www.hpc-uk.org is avaialble to the public at all times other than maintenance	

1) Worked example: Cheques in a post bag are carried across from Park House to Stannary Street, once a week. How often would the loss occur with a security impact?

1) Worked example 2: HPC's website is available on the internet 24hrs x 365 days. How often will it be attacked and breached by an internet worm?

HCPC's existing risk assessment matrix has been adapted for ISO27001 use.

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

The costs to certify with BSI to ISO27001 have been determined as indicated in the table below.

Item	Excl VAT	Incl VAT
Application fee	FREE	FREE
ISO/IEC 27001 Pre-certification Audit = 1 day	£1,017	£1,220.40
ISO/IEC 27001 Stage 1 Audit = 1 day	£1,017	£1,220.40
ISO/IEC 27001 Stage 1 Audit = 0.5 days	£673	£807.60
ISO/IEC 27001 Stage 2 Audit = 4 days	£4,068	£4,881.60
ISO/IEC 27001 Programme Management	£1,017	£1,220.40
TOTAL TO CERTIFY	**£7,792**	**£9,350.40**
Annual Audit details can be found below;		
Annual Audit = 2 days per annum	£2,034	£2,440.80
Planning Time = 1 day per annum	£1,017	£1,220.40
Annual Management Fee	£377	£452.40
TOTAL ANNUAL CHARGES	**£3,428**	**£4,113.60**

EMT have decided to progress the ISO27001 certification project, aiming for completion in this financial year as long as no major uncontrolled risks are located, and resources allow. Some other costs will be incurred with contractors to validate our Information Security Management System as it develops, prior to the BSI part of the process.

PCI-DSS related processes across the organisation are the responsibility of the Finance Department. However the BPI Department will continue to provide input to the overall process. All computer based PCI-DSS remit data has been re-engineered to be outside HCPC scope. A small amount of paper based processing is required to undertake postal international applications.

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.

The CESG (the Information Assurance arm of GCHQ) Information Assurance standard for employees with roles relating to information security will be investigated in 2013-14.

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 and IT-Governance systems has been used for existing employees and contractors over the last two years. An alternate solution will be sourced for use by employees in 2013-14 and at least one option has already been identified. An annual All Employee presentation concerning security and or risk will take place in the summer as the new “Computer Based Training” training system is rolled out.

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 2013 [Risks 2.1, 2.5]

HCPC will carry out an annual disaster recovery / business continuity test in 2013, with a predefined scenario undertaken by CDT, with the assumption that EMT are unavailable. Some members of EMT may act as observers.

5) Maintenance and availability of HCPC’s Disaster Recovery plan [Risks 2.1, 2.5]

HCPC’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 HCPC’s operations.

The Phoenix (Shadow Planner) solution has been selected as a possible solution to putting HCPC’s plan online. This system 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.

This has been deferred from the 2012-13 budget year due to other priorities. 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]

We will continue to audit the hard copy archive in Cheshire, 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. We will begin conservation of the original hand written registers in the new financial year.

An exercise to assess the condition and usefulness of documentation from the 1960's will be undertaken, and some scanning and destruction of paper copies, in line with our published retention policy will take place.

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

It is likely that transaction volumes and types will grow across HCPC. For example during the renewal of the Social Work profession thousands of calls were made into the Registrations Department each day during the last weeks of renewal activity. 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 HCPC's take up of either of the new standards are as follows. The information security standard mandates regular auditor training. This is effectively a CPD requirement. The high level training requirement is for at least two ISO27001 qualified auditors at all times. One of these can be a ISO27001 Lead Auditor.

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 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 reporting requirements to be fulfilled.

Any large scale change to the reporting technology used at HCPC will require an external resource to replicate existing reports to the new platform or reporting suite as many hundreds of report variants are maintain for various parts of the organisation.

Tasks and Projects completed in 2012-13

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 HCPC'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 2012-13 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.

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

The HCPC 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 HCPC. This service has been purchased, and training of key Operations Department members is underway.

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 HCPC. Some low level policy work and training has continued on ISO27001. The HCPC Information Security Policy was signed off by EMT in September 2010. The PCI-DSS project was 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]

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

The IT Department made changes to the background reporting software configuration over early summer 2012, which required testing and refinement of all major reports used. This was carried out satisfactorily.

Monthly reporting on behalf of the Finance Department continued whilst additional functionality is developed.

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

HCPC 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 HCPC. This is an essential requirement of the ISO27001 standard. Threats and vulnerabilities and mitigations / controls must be tracked long term by HCPC 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
- Tendering and Procurement review, and enhancement of the OJEU processes in conjunction with the Bircham Dyson Bell legal team.
- 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. This was updated in winter 2012/13 to inform the Audit Committee on progress on house keeping points.
- 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 published on the HCPC website April / May 2012
- Applications and Registration at CPSM, 1962 to 2002, report by Tom Berrie, first draft for internal circulation.
- A research report on CPSM / HCP / HCPC and its accommodation in Kennington was published in March 2013, featuring photographs of the past and current office space occupied by the organisation.
- Roy Dunn completed the Practitioner Certificate in Information Risk Management qualification in relation to the ISO27001 project.

The level of FOI reporting required by HCPC's stakeholders and the public 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 2013	Likelihood before mitigations Jan 2013	Risk Score = Impact x Likelihood	Mitigation I	Mitigation II	Mitigation III	RISK score after Mitigation Jan 2013
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	Detailed workforce plan to match workload	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	Fraud committed through IT services	Director of IT	3	3	**9**	Appropriate and proportionate access restrictions to business data. 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 HCPC	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 NetRegulate and bank statements.	Tight procedures to retrieve sensitive paper records from archive, rationalise records kept and retain sensitive current year records	Compliance with credit card record storage standards.	Low

							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**	Access is restricted to only the data that is necessary for the performance of the services.	Effective system processes including secure data transfer and remote access granted only on application and through secure methods. Physical transfer of back up tapes using specialist company with locked boxes and sign out procedure.	Data processor agreements signed by the relevant suppliers	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

17.5	Loss of physical data despatched to and held by third parties for the delivery of their services	Director of Ops and Hd of Business Process Improv	5	3	15	Data Protection/Controller agreements signed by the relevant suppliers. Use of electronic firewalls by suppliers.	Use of transit cases for archive boxes sent for scanning or copying and sign out procedures.	-	Low
17.6	Loss of Registrant personal data by the registration system (NetRegulate) application support provider in the performance of their support services (specific risk).	Director of IT and Director of Operations	5	3	15	Access to and export of Registrant data is restricted to only that which is necessary for the performance of the services.	Effective system processes including secure data transfer and remote access granted only on application and through secure methods.	Data processor side letter specifying obligations and granting a limited indemnity.	Low