Audit Committee, 15 June 2016

BSI ISO 9001 & ISO 27001 audit reports

Executive summary and recommendations

Introduction

BSI have been on site to carry out the ISO 9001:2008 recertification audit, and the surveillance audit for ISO 27001:2013

ISO 9001 report;

- one observation around whether root cause can be assigned for all reported outcomes or activities
- one opportunity for improvement, around upgrading the Facilities ticketing system, to allow direct response to emails from the system
- there was one verbal comment about matching the Strategic Objectives to the Risk Register in detail. (not documented in detail in report). Resolution of this is in progress.

ISO 27001 report;

- previous non-conformances successfully closed;
- one observation around linking Risk Assessment and the Statement of Applicability
- one observation around timeliness of carrying out post implementation reviews
- one opportunity for improvement, around indicating the level to which controls have been applied
- one minor non-conformance around lack of evidence that information in "(A 12.4.2 & A 12.4.3) Admin or Operator logs are protected from possible unauthorised changes".

HCPC successfully passed both audits.

Decision

The Audit Committee are asked to note the reports.

Resource implications

None known

Appendices

BSI Audit report ISO 9001:2008
BSI Audit report ISO 27001:2013

Date of paper

2 June 2016

Assessment Report.

The Health and Care Professions Council

Report Author **Andrew Babbs**

Visit Start Date 20/04/2016

Introduction.

This report has been compiled by Andrew Babbs and relates to the assessment activity detailed below:

Visit ref/Type/Date/Duration	Certificate/Standard	Site address
8299572 Re-certification Audit (SR Opt 1) 20/04/2016 2 day(s) Effective no. of employees : 240 Total no. of employees : 240	FS 83074 ISO 9001:2008	Health & Care Professions Council Park House 184 Kennington Park Road London SE11 4BU United Kingdom

The objective of the assessment was to ascertain the integrity of the organisation's management system over the current assessment cycle to enable re-certification and confirm the forward strategic assessment plan.

Management Summary.

Overall Conclusion

We are pleased to recommend the continuation of your certification. I would like to thank all the audit participants for their assistance and co-operation which enabled the audit to run smoothly and to schedule.

The audit objectives have been achieved and the certificate scope remains appropriate. The audit team concludes based on the results of this audit that The Health and Care Professions Council does fulfil the standards and audit criteria identified within the audit report and it is deemed that the management system continue to achieve its intended outcomes.

The audit team recommends that BSI consider the information found in this assessment report as evidence in part, of the conformity of The Health and Care Professions Council with the requirements for ISO 9001 recertification.

There were no outstanding nonconformities to review from previous assessments.

No new nonconformities were identified during the assessment. Enhanced detail relating to the overall assessment findings is contained within subsequent sections of the report.

Mandatory Requirements – Re-Certification.

Has the Recertification Review Pack been reviewed prior to the assessment by the Client Manager ?

Yes

Have all requirements of the standard been implemented?

Yes

Has the entirety of scope / processes been assessed during the current review period?

Yes

Has the certificate structure and location activities been reviewed?

Yes

Based on the recertification process, the management system continues to demonstrate the ability to support the achievement of statutory, regulatory and contractual requirements.

Where applicable, has a Technical Expert(s) been used in the Certification cycle? detail the frequency.

Complaints Received by BSI

The following details relate to complaints received by BSI relating to the clients activities during the certification period.

A complaint has been received during the current certification cycle and is currently being investigated.

Strategic Review Pack Summary

A review of the previous three year cycle has identified the following observations were raised:-

Observations
- 01/05/2015 Fitness to Practise - Compliance 8.2.2
Details: The organisation need to consider what is deemed as 'undue delay' in relation to corrective actions resulting from their internal audit process.

- 09/05/2014 Observations and Opportunities for Improvement 6.3
Details: It was observed that 'Request for Change' submissions are required to be reviewed by the CAB (Change Approval Board). However, the CAB is currently the IT Manager. Management may consider the setting up of a full CAB to review, approve and schedule all changes to the IT Infrastructure. This would then provide a more independent and objective review of a RFC's.

- 09/05/2014 Observations and Opportunities for Improvement 6.3
Details: It was observed that the request to create a new starter account within the Active Directory is requested by email. As an opportunity for improvement, all requests for new accounts and changes to existing accounts should always be documented within the 'Ticket Management System' (Absolute). This would then provide a full audit trail of the creation of the account, including any changes and additions, etc.

No non-conformities or opportunities for improvement were raised over the cycle prior to this assessment.

Progress in relation to management system objectives.

The Organisation has one clear objective as a regulator:-
To safeguard the health and well-being of persons using or needing the services of registrants
To support this the Organisation has in place a Strategic Plan with Aims and Values. This has been assessed further in the main body of this report.

Leadership, Commitment and Strategy

An open discussion was held with the Chief Executive / Regulator and Director of Operations. Commitment to the management system and drive to achieve results using the management system was evident. The position of the Organisation through its one overarching objective was reiterated and the additional support from the standards - ISO 9001 and ISO 10002 was considered

important for the Organisation to ensure processes are controlled. Change for the Organisation is controlled over longer periods of time in comparison to other companies certified to 9001.

Effectiveness of the Management System

The management system is established and is considered to have effective interactions between all elements of the system.

Impartiality Review

The following list of assessors has been utilised during the cycle which demonstrates impartiality:-

7809716 Re-certification Audit (SR Opt 1) 02/05/2013 1 Ali Mian
7885597 Continuing assessment (surveillance) 07/10/2013 1 Ali Mian
7964314 Continuing assessment (surveillance) 06/05/2014 1 Andrew Connett
8042383 Continuing assessment (surveillance) 04/11/2014 1 Lisa Clarke
8127584 Continuing assessment (surveillance) 29/04/2015 2 Andrew Babbs
8218738 Continuing assessment (surveillance) 22/10/2015 2 Ali Mian
8299572 Re-certification Audit (SR Opt 1) 20/04/2016 2 Andrew Babbs

The entirety of the scope has been covered:-
'The management and operation of The Health and Care Professions Council (HCPC) covering: Statutory professional self-regulation Reports to the Privy Council.'

The following areas assessed over the three year period:-
- Quality management system
- Staff Development and Training
- Risk register
- Work environment and infrastructure/facilities management
- Quality Assurance
- Communications
- Social Media
- Stakeholders
- Publishing
- Web & Digital
- Internal Communications
- Events
- Finance
- Invoicing & Purchase Ledger
- Management Accounts
- Procurement (purchasing and suppliers)
- Transactions
- Education
- Operations NNIW
- Operations SES
- Communications and Development
- quality assurance
- Policy and Development
- Fitness to Practice
- Adjudication
- Administration
- Assurance & Development
- Case Support
- Case Teams 1-5

- Case Teams 6-7
- Compliance
- Investigations
- HR/partner validation
- Policy
- Projects
- Registrations
- International
- UK
- CPD
- Operations
- IT
- Infrastructure
- Service support
- Secretariat
- Customer Services
- Information Governance
- Council Processes

The following days have been completed over the three year certification cycle:-

One day every six months -
- Re-certification Audit (SR Opt 1) 02/05/2013 1
- Continuing assessment (surveillance) 07/10/2013 1
- Continuing assessment (surveillance) 06/05/2014 1
- Continuing assessment (surveillance) 04/11/2014 1

Changed to two days every six months following recalculation of staff numbers versus assessment days -
- Continuing assessment (surveillance) 29/04/2015 2
- Continuing assessment (surveillance) 22/10/2015 2
- Re-certification Audit (SR Opt 1) 20/04/2016 2

The calculation does reflect the required man days at time of previous assessments and are a minimum amount of days.

Do you want the current Total assessment days / Cycle to continue ?

Yes

Justified Exclusions

Justified exclusions have been confirmed for certificate : FS 83074

details:

The system manual has identified the following exclusions from the standard:-
- 7.3 Design & development
- 7.5.5 Preservation of Product
- 7.6 Control of Monitoring and Measuring Equipment

These are considered as justified.

Areas Assessed & Findings.

Opening meeting :

An opening meeting was held and the scope for the visit discussed in relation to ISO 9001 that specifies requirements for a quality management system where an organization needs to demonstrate its ability to consistently provide product that meets customer and applicable statutory and regulatory requirements, and aims to enhance customer satisfaction through the effective application of the system, including processes for continual improvement of the system and the assurance of conformity to customer and applicable statutory and regulatory requirements.

The processes for the different types of assessments was discussed to clarify the BSI procedures for ISO certification relating to continuing assessment visits and strategic reviews. The potential outcomes and differences between the aforementioned assessments were outlined.

During the opening meeting the client confirmed awareness of the contract conditions and BSI's confidentiality statement. The assessment plan was discussed including note taking and the issue of the report. The assessment is based on sampling; all findings are identified at the time. Guides will be available and details of specific Health and Safety aspects were confirmed.

Core Management System :

The Organisation has a Quality Manual which was found dated 19/04/2016 and current copy number 0020001/0015. The organisation has an improved versioning structure within its system that started in 2010. The scope of the management system is the same as the certification of ISO 9001:2008:- 'The management and operation of The Health and Care Professionals Council (HCPC) covering: Statutory professional self-regulation, and Reports to the Privy Council. An extension to the identified locations has been noted within the manual.

The system manual has identified the following exclusions from the standard:-
- 7.3 Design & development
- 7.5.5 Preservation of Product
- 7.6 Control of Monitoring and Measuring Equipment

These are deemed as justified exclusions as the organisation do not do currently any design and development, they have no physical product that requires handling, storage or protection and there is no equipment that requires calibration.

The interactions between the processes was seen within the manual. The manual also has hyperlinks to the specific procedures which include the mandatory procedures.

The Organisation's Quality Policy was found to be dated 16/02/2016 with a version number of 0020022/003. A commitment to ISO 9001 and ISO 10002. The Policy refers to the Strategic Intent document for 2016 to 2020.

The main objectives are as follows:-
'To safeguard the health and well-being of persons using or needing the services of registrants'

in meeting this objective the Council shall:
'have proper regard to the interests of all registrants and prospective registrants and persons [using or needing the services of registrants]'

This was found to be supported by the following guiding principles:-
- Transparency
- Collaboration
- Responsiveness
- Value for money
- High quality service

The Organisation also have Aims
- Maintaining and publishing a public register of properly qualified member of the professions
- Approving and upholding high standards of education and training, and continuing good practice
- Investigating complaints and taking appropriate action
- Working in partnership with the public, and a range of other groups including professional bodies
- Promoting awareness and understanding of the aims of the Council

The Strategic Intent document is publically available via the website dated January 2016. The following strategic objectives were noted:

- Good governance
- Efficient business processes
- Effective Communication
- Evidence informed regulation
- Influence the policy agenda
- Engagement in the four countries

The Risk Register was reviewed and the top ten risks discussed. Some of the links between the Strategic Objectives and the identified Organisational risks were unclear. The scoring matrix was found to identify clearly the areas that need attention.

Performance Evaluation & Improvement :

The Organisation gathers feedback from interested parties via the website and through various other medias. A monthly report is produced for the Executive Management Team (EMT). The Customer Service feedback report for January was sampled with the following data:-
- 32 Complaints received (noted as being below average)
- 4 general feedback letters
- 2 letter from MP's
- 7 Positive feedback letters

The Organisation conducts its internal audits on a risk basis. The audit plan mirrors the main certification assessment plan. The plan also includes the Information Security Management system. Evaluations of the supply chain were found to have been included in the audit schedule. The movement of internal audits are noted as having been moved on occasion. The following audit samples were reviewed:-
- August 2015 - FTP Redactions - various actions were identified. - Corrective Actions followed to Improvement Log
- April 2016 - Facilities Management - Corrective Action traced.
- March 2016 - Registration Operations - Observations and Opportunities for Improvement reviewed

The Management Review process was seen and the flow chart references the relevant elements of the inputs and outputs for Management Review were noted. The following activities take place as part of the review process:-
- EMT Away days
- Council Away days
- Risk Management Process
- CDT Meetings
- Monthly EMT Meetings
- Committee Meetings
- Council Meetings

Sample Council Meeting minutes were seen for March 2016. There are two levels of the multi faceted review process from Strategic and Operational points of view.

This was deemed to be effective performance evaluation.

Observations.

Type	Area/Process	Clause
Observations	Performance Evaluation & Improvement	8.5.2
Scope	FS 83074	
Details:	The organisation need to consider the significance of improvements being raised and whether the root cause needs to be identified in all cases.	

Facilities Management :

The process which included a ticketing system was explained and examples of how the team had dealt with the internal clients requests and specifications was reviewed. The various levels of urgency were discussed and the ability of the Facilities team to change the priority of requests was explained and considered to improve tha accuracy of the responses and planning of works. The following tickets were sampled:-

- 102355
- 102032
- 102335

The management system was generally found to be effective, no complaints had been received for the department and at time of assessment 25 tickets were open and had been programmed for completion.

The team also explained about the preferred supplier list which again was in line with the requirements of the standard for evaluation, selection and re-evaluation.

Opportunity for improvement.

Type	Area/Process	Clause
Opportunity for improvement	Facilities Management	
Scope	FS 83074	
Details:	The Organisation may wish to consider improving the ticket system so that all correspondence is logged through the system rather than via email separately.	

Finance - Procurement & Refunds :

The Department is current reviewing the processes in relation to procurement and is considering the scope of its needs. The Organisation is subject to the OJEU process for goods and services and uses a framework to support the procurement process via Crown Commercial services. This was found to be effective for the areas assessed and supported the Facilities Teams explanation for contracted works.

The processes for Refunds was explained and demonstrated through examples for the three types of refund:-
- Cheque
- BACS
- A-BACS

The process for verification and validation was seen to be controlled and effective.

Excellent record control was demonstrated in relation to this process.

During the course of the visit logos were found to be used correctly.

Assessment Participants.

On behalf of the organisation:

Name	Position
Roy Dunn	Head of Business Process Improvement
Kayleigh Birtwistle	Quality Compliance Auditor
Marc Seale	Chief Executive & Registrar
Greg Ross-Sampson	Director of Operations
Andy Gillies	Director of Finance
Stephanie Hewitt	Finance Officer
Robert Pope	Interim Facilities Manager
Charlotte Bennett	Facilities Officer

The assessment was conducted on behalf of BSI by:

Name	Position
Andrew Babbs	Team Leader

Continuing Assessment.

The programme of continuing assessment is detailed below.

Site Address	Certificate Reference/Visit Cycle	
Health & Care Professions Council Park House 184 Kennington Park Road London SE11 4BU United Kingdom	FS 83074	
	Visit interval:	6 months
	Visit duration:	2 Days
	Next re-certification:	01/04/2019

Re-certification by Strategic Review will be conducted on completion of the cycle, or sooner as required. The review will focus on the strengths and weaknesses of your Management System.

Certification Assessment Plan.

HEALTH-0047125084-000|FS 83074

Business area/Location		Visit1	Visit2	Visit3	Visit4	Visit5	Visit6	Visit7	Visit8
	Date (mm/yy):	04/16	10/16	01/17	04/17	10/17	04/18	10/18	04/19
	Duration (days):	2.0	2.0	1.0	2.0	2.0	2.0	2.0	2.0
Quality management system - key controls - see appendix for full listing*		X	X		X		X		X
Staff Development and Training			X						
Purchasing/supplier evaluation (see Procurement)		X							X
Risk register		X	X		X		X		X
Work environment and infrastructure/facilities management		X							X
Senior management interview		X							X
Strategic review - using pack of information supplied by BSI		X							X
Communications - Social Media					X		X		
Communications - Stakeholders					X		X		
Communications - Publishing					X		X		
Communications - Web & Digital					X		X		
Communications - Internal Communications					X		X		

Communications - Events				X		X		
Finance - Procurement (purchasing and suppliers)	X							X
Finance - Transactions	X							X
Finance - Forecasting								X
Education - Policy, Communications and Development		X						
Education - Quality Assurance		X						
Education - Operations		X						
Fitness to Practice - Adjudication						X		
Fitness to Practice - Case Reception & Triage						X		
Fitness to Practice - Case Preparation & Conclusion						X		
Fitness to Practice - Operations						X		
Fitness to Practice - Investigations						X		
HR/partner validation		X						
Policy		X						
Projects							X	
Registrations - International				X				
Registrations - EMR				X				
Registrations - UK				X				
Registrations - CPD							X	
Registrations - Operations							X	

Registrations - Quality Assurance							X	
IT - Infrastructure							X	
IT - Service support							X	
Secretariat - Information Governance		X					X	
Secretariat - Council Processes		X					X	
Readiness Review - Transition to ISO 9001:2015			X					

Next Visit Plan.

Visit objectives:

The objective of the assessment is to conduct a surveillance assessment and look for positive evidence to ensure the elements of the scope of certification and the requirements of the management standard are effectively addressed by the organisation's management system and that the system is demonstrating the ability to support the achievement of statutory, regulatory and contractual requirements and the organisations specified objectives, as applicable with regard to the scope of the management standard, and to confirm the on-going achievement and applicability of the forward strategic plan.

The scope of the assessment is the documented management system with relation to the requirements of ISO 9001:2008 and the defined assessment plan provided in terms of locations and areas of the system and organisation to be assessed.

Date	Assessor	Time	Area/Process	Clause
DAY 1	Andrew Babbs	09.00	Opening Meeting	
			Education - Policy, Communications and Development	
			Education - Quality Assurance	
		12.30	Lunch	
			Education - Operations	
			HR/partner validation	
		15.00	Report Preparation	
		16.30	Interim Meeting	
DAY 2	Andrew Babbs	09.00	Interim Meeting	
			Policy	
			Secretariat - Information Governance	
			Secretariat - Council Processes	
		12.30	Lunch	
			Quality management system - key controls - see appendix for full listing*	
		14.30	Report Preparation	
		16.00	Closing Meeting	

Please note that BSI reserves the right to apply a charge equivalent to the full daily rate for cancellation of the visit by the organisation within 30 days of an agreed visit date. It is a condition of Registration that a deputy management representative be nominated. It is expected that the deputy would stand in should the management representative find themselves unavailable to attend an agreed visit within 30 days of its conduct.

Scope of Certificate FS 83074 (ISO 9001:2008).

Main Scope

The management and operation of The Health and Care Professions Council (HCPC) covering: Statutory professional self-regulation Reports to the Privy Council.

The scope has been confirmed as correct.

Location	Scope
Health & Care Professions Council Park House 184 Kennington Park Road London SE11 4BU United Kingdom HEALTH-0047125084-000	Main Certificate Scope applies.

Notes.

The assessment was based on sampling and therefore nonconformities may exist which have not been identified.

If you wish to distribute copies of this report external to your organisation, then all pages must be included.

BSI, its staff and agents shall keep confidential all information relating to your organisation and shall not disclose any such information to any third party, except that in the public domain or required by law or relevant accreditation bodies. BSI staff, agents and accreditation bodies have signed individual confidentiality undertakings and will only receive confidential information on a 'need to know' basis.

'Just for Customers' is the website that we are pleased to offer our clients following successful registration, designed to support you in maximising the benefits of your BSI registration - please go to www.bsigroup.com/j4c to register. When registering for the first time you will need your client reference number and your certificate number (47125084/FS 83074).

This report and related documents is prepared for and only for BSI's client and for no other purpose. As such, BSI does not accept or assume any responsibility (legal or otherwise) or accept any liability for or in connection with any other purpose for which the Report may be used, or to any other person to whom the Report is shown or in to whose hands it may come, and no other persons shall be entitled to rely on the Report.

Should you wish to speak with BSI in relation to your registration, please contact our Customer Engagement and Planning:

Customer Services
BSI
Kitemark Court,
Davy Avenue, Knowlhill
Milton Keynes
MK5 8PP

Tel: +44 (0)845 080 9000

Email: MK.Customerservices@bsigroup.com

Regulatory Compliance.

BSI conditions of contract for this visit require that BSI be informed of all relevant regulatory non-compliance or incidents that require notification to any regulatory authority. Acceptance of this report by the client signifies that all such issues have been disclosed as part of the assessment process and agreement that any such non-compliance or incidents occurring after this visit will be notified to the BSI client manager as soon as practical after the event.

Expected Outcomes for Accredited Certification.

What accredited certification means:

The accredited certification process provides confidence that the organization has a management system that conforms to the applicable requirements of the certified standards covered within this assessment and scope of certification.

What accredited certification does not mean:

It is important to recognize that certification defines the requirements for an organization's management system, not for its products or services. It does not imply that the organization is providing a superior product or service, or that the product, service or performance itself is certified as meeting the requirements of an ISO standard or specification or that the organisation can guarantee 100% product, service or performance conformity, though this should of course be a permanent goal.

Assessment Report.

Health & Care Professions Council

Introduction.

This report has been compiled by Kwadwo Anim-Appiah and relates to the assessment activity detailed below:

Visit ref/Type/Date/Duration	Certificate/Standard	Site address
8350424 Continuing Assessment (Surveillance) 26/04/2016 2 day(s) Effective no. of employees : 240 Total no. of employees : 240	IS 600771 ISO/IEC 27001:2013	Health & Care Professions Council Park House 184 Kennington Park Road London SE11 4BU United Kingdom

The objective of the assessment was to conduct a surveillance assessment and look for positive evidence to ensure that elements of the scope of certification and the requirements of the management standard are effectively addressed by the organisation's management system and that the system is demonstrating the ability to support the achievement of statutory, regulatory and contractual requirements and the organisations specified objectives, as applicable with regard to the scope of the management standard, and to confirm the on-going achievement and applicability of the forward strategic plan and where applicable to identify potential areas for improvement of the management system.

The scope of the assessment is the documented management system with relation to the requirements of ISO 27001:2013 and the defined assessment plan provided in terms of locations and areas of the system and organisation to be assessed.

Management Summary.

Overall Conclusion

I would like to thank all the audit participants for their assistance and co-operation which enabled the audit to run smoothly and to schedule.

The audit objectives have been achieved and the certificate scope remains appropriate. The auditor concludes based on the results of this audit that Health & Care Professions Council does fulfil the standards and audit criteria identified within the audit report and it is deemed that the management system continue to achieve its intended outcomes.

The auditor recommends that BSI consider the information found in this assessment report as evidence in part, of the conformity of Health & Care Professions Council with the requirements for ISO 27001:2013 continued certification.

It was commendable to note that information security training has been pushed out to 96% of employees including contractors as well as 94% of the HCPC's 600 partners. Measures have been taken to ensure that reminders on the need to lock unattended computers are printed on mouse pads and cup covers. Information security champions were seen to have been trained to help disseminate information security requirements within the organisation. Employees demonstrated information security awareness. Non-conformities were seen to have been dealt with as required. Overall, very good effort made considering that the certificate was issued just 10 months ago.

Corrective actions with respect to nonconformities raised at the last assessment have been reviewed and found to be effectively implemented.

A minor nonconformity requiring attention was identified. This, along with other findings, is contained within subsequent sections of the report.

A minor nonconformity relates to a single identified lapse, which in itself would not indicate a breakdown in the management system's ability to effectively control the processes for which it was intended. It is necessary to investigate the underlying cause of any issue to determine corrective action. The proposed action will be reviewed for effective implementation at the next assessment.

Areas Assessed & Findings.

Opening Meeting including changes to the management system : 4

The formal opening meeting included the objective of the assessment, methodology and terminology used, confidentiality, number of staff in scope, purchase order details (not required), and the agreed assessment plan.

The scope was confirmed as unchanged. No major changes were noted, however it was noted the adjudications team which forms part of fitness to practice has moved into a new building at the end of Kennington Road. The address is 405 Kennington Road, London, SE11 4PT.

BSI has received a complaint from one of HCPC's registrants complaining about the Fitness to Practice process. The complaint is being processed by BSI. A letter dated 24th March 2016 with reference CCF010 from BSI was evidenced indicating that an investigation on the matter will take place on 31st May 2016. This will be carried out by Andrew Babbs.

Performance Monitoring & Measurement / ISMS Objectives / NC Closeouts : 9.1, 6.2

The Operations Directorate Report to the Council was reviewed and noted that the objectives set for the ISMS were on target or been achieved. HCPC had achieved 96% training as at February 2016. As at March 2016, 94% of the 600 partners had undergone information security training. Similarly, 96% of the employees including contractors had undergone information security training. Service availability is at 100% although there were dips in June 2015 and January 2016. HCPC successfully got certified to ISO 10002:2014 (Customer Satisfaction Management System). A certificate was issued to HCPC on 7th April 2016.

The 2 outstanding NCs were closed out successfully.

Documents reviewed included:
1. DOC A3 Effectiveness Measures
2. Audit Schedule

ISMS Monitoring and Improvement; Internal Audit; Management Review; Corrective Action / Incident Management : 9.2, 9.3, 10

It was noted that HCPC had carried out audits for the following standards: ISO 27001, ISO 9001 and ISO 10002. Audit schedule reviewed now covers three standards. ISO 27001 audit reports were reviewed and seen to be well maintained. NCs and Observations were seen to have been captured into HCPC's Improvement Log and its incident/audit reports. The Improvement Log reviewed showed all findings, root causes and subsequent actions taken as well as incidents. It was further noted that IT Governance (3rd party consultants) was brought in March 2016 to carry out an internal audit on behalf of HCPC. The audit covered all controls and management clauses of ISO 27001.

HCPC now has in place a Management Review Diagram that explains how and which parts of the organisation is responsible for the various inputs/outs for management reviews in order to meet the requirements of clause 9.3. IT Governance (3rd Party consultants) is then brought in to review the whole ISMS. However, the Executive Management Team (made up CEO and Directors) undertake

monthly meetings also reviews audit findings. 6 monthly information security reports are also generated and presented to the council.

HCPC maintains incidents within its Improvement Log as well as incident forms and reports. Information security incidents are managed by the Information Governance Manager. The organisation maintains a 24 hour turn around however if there is the need to urgently action an incident a meeting will be conveyed ASAP which involves the EMT. Incident rating is maintained for all incidents recorded and assessed which is based on the ICO's requirements. Lessons learned are reviewed at the EMT monthly meetings as well as a 6 monthly review of recommendations are evaluated accordingly for effectiveness.

Incidents sampled:
IIR34.2016 - Signed for post lost internally (22/04/2016)
IIR17.2016 - Unredacted Information (09/03/2016)
IIR25.2016 - Information belonging to another registrant sent to a UK applicant in error (29/03/2016)
IIR9.2016 - Incomplete redaction of information (09/02/2016)

All incidents reviewed were seen to have been dealt with accordingly.

Documents reviewed included:
1. Audit Schedule
2. REC MS2 Internal Audit Report - Tidy Desk Comms (Feb 2016)
3. Supplier Authorisation Form (for destruction)
4. REC MS2 Internal Audit Report - Fire Evacuation/ Smoke Sensors (Feb 2016)
5. REC MS2 Internal Audit Report - FTP Investigations (Feb 2016)
6. REC MS_4A Improvement Log v1.3
7. ISMS REC MS-2A Internal Report Audit Lead (03/03/2016) - ITG Audit
8. Monthly Executive Management Team Meeting (29/03/2016)
9. Monthly Executive Management Team Meeting (26/02/2016)-Includes 6 Monthly Information Security Report
10. Information Incident Reports

Risk Assessment / Risk Treatment & SOA : 6, 8

HCPC is moving away from [redacted] and has in place a new risk assessment and treatment process captured on a spreadsheet. The updated risk management process was reviewed and seen to now reflect HCPC's risk levels which are Medium, Low and High. [redacted] only allowed the organisation to rate its risks as Low or High only. The process is still modelled on a 5x5 scoring matrix. HCPC was having challenges with [redacted] and felt was not user friendly when it comes to producing reports for the EMT Meetings. Information risks have been categorised to cover all departments as well as strategic risks.

Sampled risks:
#2.7 Interruption to electricity power supply (High)
#17.9 Loss of ISO27001:2013 certification (Medium)
#5.1 Software Virus Damage (Low)
#5.6 Data Service Disruption (Low)

All risks reviewed were seen to have been mitigated as per HCPC's process and standard requirements.

The SOA reviewed was at version 1.3 and dated 02/03/2016. No exclusions were noted. Justifications for inclusions were in place with evidence reference documents.

Documents reviewed included:
1. DOC A2 Risk Management v1.3 (28/03/2016)

2. 20160307 ADTSTRAT Risk Treatment Plan Mar 2016 Assurance Map
3. DOC Statement of Applicability v1.3 (02/03/2016)

Observations.

Type	Area/Process	Clause
Observations	Risk Assessment / Risk Treatment & SOA	6.1.2
Scope	IS 600771	
Details:	HCPC currently considers the risks associated with the loss of CIA implicitly as part of the process. HCPC must ensure that consideration of CIA is explicit which will in turn help risk owners during the risk assessment and treatment process.	

Opportunity for improvement.

Type	Area/Process	Clause
Opportunity for improvement	Risk Assessment / Risk Treatment & SOA	6.1.3
Scope	IS 600771	
Details:	HCPC's SOA was reviewed and seen to indicate that all controls have been applied (implemented). As an opportunity for improvement, the organisation might want to show which of the controls have been fully or partially implemented to help measure the maturity of the controls going forward.	

Business Continuity : A.17

A flooding event that occurred as a result of a burst water main on Kennington Road and as such the BCP was invoked. This occurred on 29th June 2015. Whilst the BCP procedures was being followed, unfortunately an Executive Member of the organisation and also a key member of the BCP team was unwell and as such this heightened the scenarios that were used. Pictures of the flooding which was seen have turned the Kennington Road into a "river". Measures taken were reviewed which includes the shutting down of the IT department and barricading the basement with sand bags were seen in the form of pictures of the event. Workers were contacted and asked to work from home. Backup power was run from the Mezzainine level of 20 Stannary Street to the server room. This was also used to power the UPS as well. Recommendations coming out of the BCP invocation were reviewed and seen to be appropriate and it was further noted that some of the recommendations have been implemented. HCPC is currently testing "Shadow Planner" which allows key employees to access contact details and the BCP offline using their Smartphones (Blackberry Devices). Devices are encrypted. Shadow Planner was demonstrated and seen to be comprehensive.

Next planned test will be based on the Shadow Planner. Planned test scenario scheduled for June 2016 was evidenced.

Documents reviewed included:
1. DOC A17 Business Continuity Management v1.3 dated 29/03/2016
2. 20150729 EMT RPT Flooding Event - Kennington Park Road (BCP Test Report)
3. REC.MS2 Internal Audit Report - BCM Planning Application Oct 2015
4. 20160311-HCPC BCM-DR Test Scenario

Operations Security (IT Department) : A.12

The IT team is split into support and infrastructure sub-teams, however they are some cross over functions. Functional separation of tasks exists within the department. The service support team is responsible also for the change management process and lends support for major IT projects within the organisation. Restrictions are in place to prevent installation of applications on the systems. Laptop hard drives are encrypted and similarly, data stored on desktops are hidden on the network and as such should the desktop be stolen no data could be accessed. Mobile devices can be wiped remotely. CD and USB drives are disabled for data storage.

HCPC undertakes a weekly CAB meeting which involves the functional heads of the IT team as well as the change requester and the business/system owner. System owner approval is a requirement. Similarly, it was noted changes require implementation plans, test plans and back out plans. Impact on DR/Business Continuity as well as information security implications were seen to have been considered in changes sampled. A master list is also maintained for all changes. HCPC has 3 types of changes and these are Normal, Standard and Emergency Changes.

Sampled changes:
RFC No. 20160012 - Demote HCPCDC01 and HCPCDC01 (29/01/2016)
RFC No. 20150128 - HCPC Website Education Data API UAT DR3 (30/10/2015)

Secure print process is in place. Two forms of backup are implemented and these are on virtual servers and data. Tapes are stored on the premises, however these are collected by a 3rd party on a monthly basis. Backup schedules are in place for backing up to data storage. Backups are done on a daily basis and 15 minutes passive backup is undertaken. Shadow Copies are done twice a day which is another defence in depth being applied. Full backup to disk is implemented on monthly and weekends with differential incremental daily backups. Last night's backup was successful and this was evidenced. Backup test restores were seen.

Message labs are used for control of incoming messages. Anti-virus and client based firewalls are in place and such protection is provided using Symantec Endpoint Protection Manager. Signatures are updated on a daily basis. Tripwire is the log event manager tool used to monitor system administrator activities. Similarly, ManageEngine Applications Manager is used to monitor services, events and the servers. The following were seen to be monitored: memory, disk space, CPU utilisation. File integrity is monitored too.

Documents reviewed included:
1. Completed Request For Change Forms
2. Change Process Diagram
3. Backups Restores

Observations.

Type	Area/Process	Clause
Observations	Operations Security (IT Department)	A12.1.2
Scope	IS 600771	
Details:	HCPC must ensure that the elapse time between change implementation and the post change reviews are clearly specified.	

HR Security : A.7

Roles identified are advertised either internally or with 3rd party agencies/job boards. Job descriptions are reviewed on annual basis or at the point before recruitment. Applications are assessed by members of a panel and shortlisted for interviews. Offer letter is sent together with IT Policy, data Handling and Email Guidance, Access to Register (depending on role) as well as code of conduct and Behaviour. Background checks carried out includes:

- References
- Right to work in the UK
- Qualifications
- Criminal Checks (depending on role)
- Employment History (3 years)

HR System currently used is based Lotus Notes however this will be replaced going forward. Notifications of the new starter and their role is sent to IT for system account creation. Induction process was reviewed and seen to be well maintained. The induction training includes information security. Similarly, departmental inductions inductions are are also given which includes training from the IT department and Business Process Improvement Department. The slides reviewed were seen to be suitable. Termination procedures were reviewed. A record each for a recent starter and leaver were reviewed and seen to be well maintained. Disciplinary procedures were seen to be in place.

Documents reviewed included:
1. New Employee Checklist
2. Induction Notes
3. Induction Checklist
4. Information Security Training Slides
5. Starters and Leavers Forms
6. Contract of Employment (template)

Awareness Sampling: Fitness to Practise/Registrations/Facilities :

The Case Manager for FTP was interviewed and she had a firm understanding of how information security requirements relate to the everyday workings of the Fitness to Practice (FTP) department. Case handling procedures were reviewed and it was noted that the department has in place FTP Operational Guidance (FOG) on key processes and procedures. As such the FTP Operational Guidance - Confidentiality and Information Security was reviewed and found to be comprehensive as it captures the below:
- Redaction process for PII
- Confirming identity of callers
- Information Security related incidents (referred to the Information Governance Manager)
- Handling of bundles
- Sending of information to panel members or registrants or receipt of information (Default position is to send bundles by post (special delivery/signed for), however these can be sent electronically in an encrypted format through the Fitness to Practice (FTP) system.

Registration process was reviewed and in particular the renewal process. The software DocXP was demonstrated which serves as a Data/Character Recognition software. Similarly, Semafone is the software used to mask credit/debit account details. Only authorised personnel within the department have access to registration systems. Different access levels does exist. Authentication and activation codes are sent in parts to avoid interception and unauthorised access. NetRegulate is the register in use.

The facilities team were interviewed and were able to demonstrate their awareness on Information security requirements related to their role. The team confirmed the starters and leavers process for access card issuance/deletion as noted during the HR Security assessment earlier on during the day. HCPC's access card management tool was demonstrated and seen to be restricted to only 2 people within the department in addition to a systems engineer from the vendor and an in-house IT personnel for support purposes. Card access permission levels dependent on role were seen to be in place. The starters and leavers process pertaining to access card issuance/deletion were demonstrated.

Overall, all employees interviewed showed awareness of information security requirements in relation to their role as well as what is expected of them in general terms. They were able to point out where information security related policies are held and had a firm

understanding of the information security incidents reporting requirements. All employees interviewed were noted to have been through HCPC's information security training. Employees interviewed had varying experiences and length of service.

Documents reviewed included:
1. FTP Operational Guidance - Confidentiality and Information Security
2. DOCXP
3. Semafone

Closing Meeting :

The closing meeting was conducted and the report findings summarised satisfactorily to those present. No comments on the report were received. The BSI standard approach including confidentiality, nature of sampling, appeals process (if required), and any forward actions following this assessment were confirmed. The next visit planning arrangements were reviewed and confirmed.

During the course of the visit logos were found to be used correctly.

Minor Nonconformities Raised at Last Assessment.

Ref	Area/Process	Clause
1193099N1	ISMS policy and procedures, internal audits, corrective action / Management review and monitoring of effectiveness of ISMS / Incident management	10.1
Scope	IS 600771	
Statement of non conformance:	Non-conformity and observations raised in previous assessment not captured	
Requirements:	Nonconformity and corrective action When a nonconformity occurs, the organization shall: a) react to the nonconformity, and as applicable: 1) take action to control and correct it; and 2) deal with the consequences; b) evaluate the need for action to eliminate the causes of nonconformity, in order that it does not recur or occur elsewhere, by: 1) reviewing the nonconformity; 2) determining the causes of the nonconformity; and 3) determining if similar nonconformities exist, or could potentially occur; c) implement any action needed; d) review the effectiveness of any corrective action taken; and e) make changes to the information security management system, if necessary. Corrective actions shall be appropriate to the effects of the nonconformities encountered. The organization shall retain documented information as evidence of: f) the nature of the nonconformities and any subsequent actions taken, and g) the results of any corrective action.	
Objective Evidence:	HCPC's improvement log (corrective action log) was reviewed. It was seen to be used as a central repository for incidents, non-conformities and observations. However, HCPC failed to capture the nonconformity and observation raised during the stage 1 assessment. HCPC must ensure that a history of all NCs raised, root cause/lessons learned are captured. Documented information of the above must be	

	retained including any subsequent actions taken.
Actions:	HCPC's REC MS_4A Improvement Log v1.3 was reviewed and it was noted that all NCs raised at both Stage 1 and 2 assessments have been logged accordingly with root causes and their respective corrective actions. Root Cause: NC not captured at time of audit publication or corrective action
Closed?:	Yes

Ref	Area/Process	Clause
1193099N2	Physical Security	A11.2.9
Scope	IS 600771	
Statement of non conformance:	The Tidy Desk Policy/1.1/28.04.2015 was not seen to have been effectively implemented.	
Requirements:	Clear desk and clear screen policy A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.	
Objective Evidence:	During the visit in the facilities two unattended working stations were noted without applying screen lock as per Policy requirements A11.2.9 Tidy Desk Policy/1.1/28.04.2015 / 5.3 "All devices including mobiles laptops should be locked when not in use" & 7.15 "If you intend to leave any computer switched on and unattended in the office at anytime you must lock your computer screen".	
Actions:	HCPC has now in place fully trained Information Security Champions. Mouse pads and cup covers printed with information security tips have been distributed to help remind employees of the need to log off or lock computers when unattended. The Tidy Policy has been amended requiring computers to be locked if they are to be left unattended for 10 minutes (and not in sight). Computers (whilst in sight) can be left unattended to retrieve printed materials. Root Cause: Failure to adhere to Tidy Desk Policy	
Closed?:	Yes	

Minor Nonconformities Arising from this Assessment.

Ref	Area/Process	Clause
1325464N1	Operations Security (IT Department)	A12.4.3
Scope	IS 600771	
Statement of non conformance:	No evidence on how information logs are protected from possible unauthorised changes	
Requirements:	Administrator and operator logs Control System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.	
Objective Evidence:	During the assessment it was noted that logs collected are deleted every now and then to free up disk space. These are undertaken by any member of the IT infrastructure sub-team who all have admin credentials. No control was evidenced as to how HCPC protects logs from unauthorised changes or the possibility of system administrators deleting any trace of unauthorised activities from the logs as part of the routine deletion process. There was no evidence on how the impact of such deletion tasks coupled with no restrictions of possible changes which can be made by those with admin credentials within the organisation has been considered. This NC should be read in conjunction with A.16.1.7.	

Assessment Participants.

On behalf of the organisation:

Name	Position
Roy Dunn	Head of Business Process Improvement
Kayleigh Birtwistle	Quality Compliance Auditor
Claire Amor	Information Governance Manager
Rick Welsby	IT Support Manager
Jason Roth	Infrastructure Manager
Kim Wilcox	HR Manager
Katia Vandenbrouke	Case Team Manager - FTP
Dushyan Ashton	Registration Manager
Tony Woodham	Facilities Officer
Charlotte Bennett	Facilities Officer
Abubacarr Jagana	Facilities Officer
Marc Seale	Chief Executive & Registrar

The assessment was conducted on behalf of BSI by:

Name	Position
Kwadwo Anim-Appiah	Team Leader

Continuing Assessment.

The programme of continuing assessment is detailed below.

Site Address	Certificate Reference/Visit Cycle	
Health & Care Professions Council Park House 184 Kennington Park Road London SE11 4BU United Kingdom	IS 600771	
	Visit interval:	12 months
	Visit duration:	2 Days
	Next re-certification:	01/04/2018

Re-certification will be conducted on completion of the cycle, or sooner as required. An entire system re-assessment visit will be required.

Certification Assessment Plan.

HEALTH-0047125084-000|IS 600771

		Visit1	Visit2	Visit3	Visit4	Visit5	Visit6
Business area/Location	**Date (mm/yy):**	03/15	05/15	04/16	04/17	04/18	04/18
	Duration (days):	2	4.5	2	2	4.5	1
Stage 1 Assessment		X					
Stage 2 Assessment			X				
Continuing Assessment				X	X		
Triennial Recertification						X	
Context of the Organisation, Scope and Policy		X	X			X	
Leadership and Commitment		X	X			X	
Planning and Resources		X	X			X	
Human Resource Security			X	X		X	
Control of Documents and Records		X				X	
Objectives / Performance Monitoring & Measurement		X	X	X	X	X	
Internal Audit, Corrective Actions, Management Review		X	X	X	X	X	
Supplier Relationships		X	X		X	X	
Risk Assessment, Risk Treatment, Statement of Applicability		X	X	X	X	X	
Compliance: Legal and Other Requirements		X	X		X	X	
Security Incident Management		X	X	X	X	X	
Access Control & Cryptography		X	X		X	X	
Physical and Environmental Security		X	X		X	X	
Asset Management			X			X	
Operations Security			X	X		X	
Communications Security			X		X	X	
System Acquisition, Development and Maintenance			X		X	X	
Business Continuity		X	X	X		X	
Registrations (Awareness Sampling)			X	X		X	
Fitness to Practise (Awareness Sampling)			X	X		X	
Policy & Standards (security awareness sampling)			X		X	X	

Education Team (security awareness sampling)		X		X	X	
Finance Team (security awareness sampling)		X			X	
Communications Team (security awareness sampling)		X			X	
Project Management Team (security awareness sampling)		X		X	X	
Programme Management (additional 1 day to review the next 3 year cycle)						X

Next Visit Plan.

Visit objectives:

CAV

The objective of the assessment is to conduct a surveillance assessment and look for positive evidence to ensure the elements of the scope of certification and the requirements of the management standard are effectively addressed by the organisation's management system and that the system is demonstrating the ability to support the achievement of statutory, regulatory and contractual requirements and the organisations specified objectives, as applicable with regard to the scope of the management standard, and to confirm the on-going achievement and applicability of the forward strategic plan.

The scope of the assessment is the documented management system with relation to the requirements of ISO 27001:2013 and the defined assessment plan provided in terms of locations and areas of the system and organisation to be assessed.

Date	Assessor	Time	Area/Process – Day 1	Clause
12/04/2017	Kwadwo Anim-Appiah	09:00	Opening Meeting including changes to the management system	
		09:15	Review of previous report/NC Closeout	
		09:30	Performance Monitoring & Measurement / ISMS Objectives / Compliance	9.1, 6.2, A.18
		10:00	ISMS Monitoring and Improvement; Internal Audit; Management Review; Corrective Action / Incident Management	9.2, 9.3, 10, A.16
		11:00	Risk Assessment / Risk Treatment & SOA /Asset Management	6, 8, A.8
		12:00	Supplier Relationships	A.15
		12:45	**Lunch**	
		13:30	Business Continuity	A.17
		14:30	Physical & Environmental Security	A.11
		15:30	Report Write-up (offsite)	
Date	**Assessor**	**Time**	**Area/Process – Day 2**	**Clause**

13/04/2017	Kwadwo Anim-Appiah	9:00	Update Meeting	
		9:15	Access Control & Cryptography	A.9
		10:15	Communications Security	A.13
		11:15	System Acquisition, Development and Maintenance	A.14
		12:15	Education Team (Awareness Sampling)	A.7.2.2
		12:45	**Lunch**	
		13:30	Policy & Standards (security awareness sampling)	A.7.2.2
		14:15	Project (Awareness Sampling)	A.7.2.2
		15:15	Report Preparation	
		16:30	Closing Meeting	

Please note that BSI reserves the right to apply a charge equivalent to the full daily rate for cancellation of the visit by the organisation within 30 days of an agreed visit date. It is a condition of Registration that a deputy management representative be nominated. It is expected that the deputy would stand in should the management representative find themselves unavailable to attend an agreed visit within 30 days of its conduct.

Scope of Certificate IS 600771 (ISO/IEC 27001:2013).

Main Scope

The management and operation of the Health & Care Professions Council (HCPC) covering statutory professional self-regulation, and reports to the Privy Council. This is in accordance with the Statement of Applicability version 1.3 dated March 2016.

The scope has been confirmed as correct.

Location	Scope
Health & Care Professions Council Park House 184 Kennington Park Road London SE11 4BU United Kingdom HEALTH-0047125084-000	Main Certificate Scope applies.

Notes.

The assessment was based on sampling and therefore nonconformities may exist which have not been identified.

If you wish to distribute copies of this report external to your organisation, then all pages must be included.

BSI, its staff and agents shall keep confidential all information relating to your organisation and shall not disclose any such information to any third party, except that in the public domain or required by law or relevant accreditation bodies. BSI staff, agents and accreditation bodies have signed individual confidentiality undertakings and will only receive confidential information on a 'need to know' basis.

'Just for Customers' is the website that we are pleased to offer our clients following successful registration, designed to support you in maximising the benefits of your BSI registration - please go to www.bsigroup.com/j4c to register. When registering for the first time you will need your client reference number and your certificate number (47125084/IS 600771).

This report and related documents is prepared for and only for BSI's client and for no other purpose. As such, BSI does not accept or assume any responsibility (legal or otherwise) or accept any liability for or in connection with any other purpose for which the Report may be used, or to any other person to whom the Report is shown or in to whose hands it may come, and no other persons shall be entitled to rely on the Report.

Should you wish to speak with BSI in relation to your registration, please contact our Customer Engagement and Planning:

Customer Services
BSI
Kitemark Court,
Davy Avenue, Knowlhill
Milton Keynes
MK5 8PP

Tel: +44 (0)845 080 9000

Email: MK.Customerservices@bsigroup.com

Regulatory Compliance.

BSI conditions of contract for this visit require that BSI be informed of all relevant regulatory non-compliance or incidents that require notification to any regulatory authority. Acceptance of this report by the client signifies that all such issues have been disclosed as part of the assessment process and agreement that any such non-compliance or incidents occurring after this visit will be notified to the BSI client manager as soon as practical after the event.