Audit Committee, 14 June 2017

BSI ISO27001:2013 audit

Executive summary and recommendations

Introduction

BSI have been on site to carry out the ISO27001:2013 Continuing Assessment Visit audit. This is carried out on an annual basis.

- HCPC have been recommended for ongoing certification
- There are five minor non conformities, namely
    - Document listing Legal requirements REC18.1 was incorrectly dated (resolved immediately) page 13
    - Annex A controls used for information risks in the Risk Register and Risk Treatment plan not listed in full (also maps to Statement of Applicability) page 13
    - User access rights not monitored on a regular basis (annual) page 14
    - Penetration testing results evidence of internal risk assessment to internal standard not documented, and results not listed in the improvement log page 15
    - Controls relating to internal development incorrectly logged as being used, (and no evidence of their use being available) page 16.
- Resolutions for each of the above non conformances will be determined with asset owners. All n/c's must be resolved and evidence created prior to the recertification audit in 2018. Failure to comply would result in an automatic Major Non conformity.
- A report on the proposed resolutions will be discussed at EMT as soon as possible, to ensure all required actions have maximum time to be addressed and can be closed off well before the next audit.
- The next annual recertification audit will take place on April 16th,17th, 18th,19th with half a day write up off site. This will be a recertification visit.

Decision

The Audit Committee are asked to discuss the report.

Resource implications

None known

Appendices
BSI Audit report ISO27001:2013 – April 2017

Date of paper
18 April 2017

Assessment Report

Health & Care Professions Council

Assessment dates	12/04/2017 to 13/04/2017
Assessment location	London (000)
Report Author	Kwadwo Anim-Appiah
Assessment Standards	ISO/IEC 27001:2013

Table of contents

Executive Summary

This assessment was HCPC's 2nd Continuing Assessment Visit (CAV) and it was commendable to note that the outstanding Minor Non-Conformity (NC) had been dealt with as required. HCPC was seen to have acquired a new software "Password Manager Pro (PMP)" to resolve the NC raised for not protecting logs as required by the standard. Administrator logs cannot be tampered with by administrators as required by the standard. It was also commendable to note that staff interviewed had clear understanding of information security requirements and how these relate to their role. However, in this assessment, 5 Minor NCs were raised and further details can be found within the relevant section in this report. These will be reviewed at the next assessment which will be HCPC's recertification assessment.

Assessment objective, scope and criteria

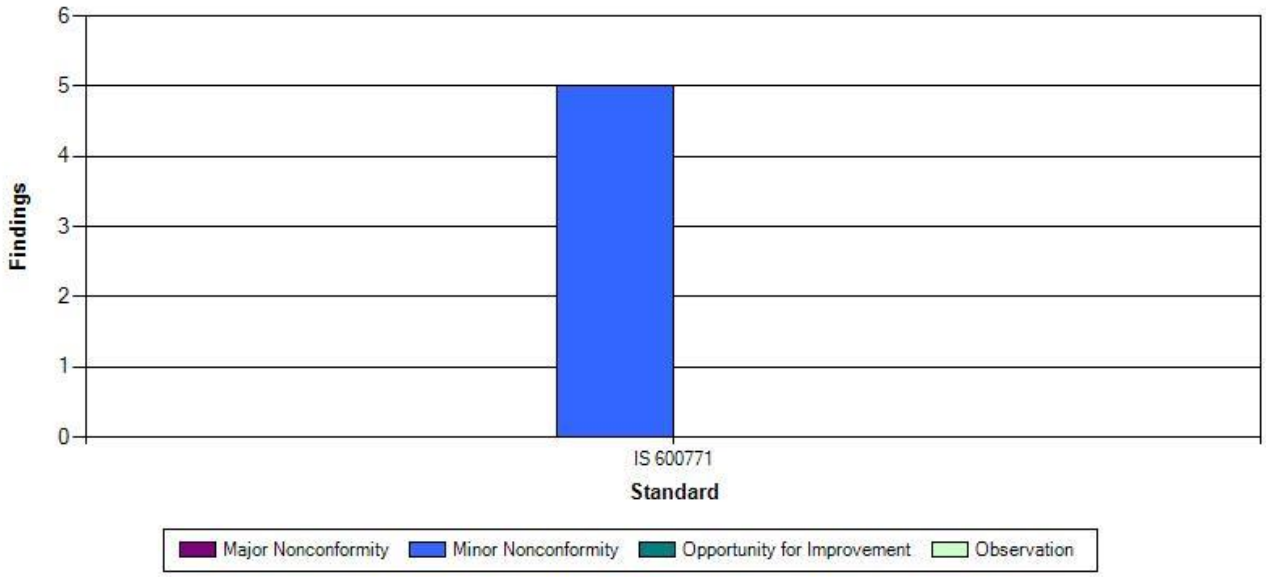
The objective of the assessment was to conduct a surveillance assessment and look for positive evidence to ensure that elements of the scope of certification and the requirements of the management standard are effectively addressed by the organisation's management system and that the system is demonstrating the ability to support the achievement of statutory, regulatory and contractual requirements and the organisation's 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.

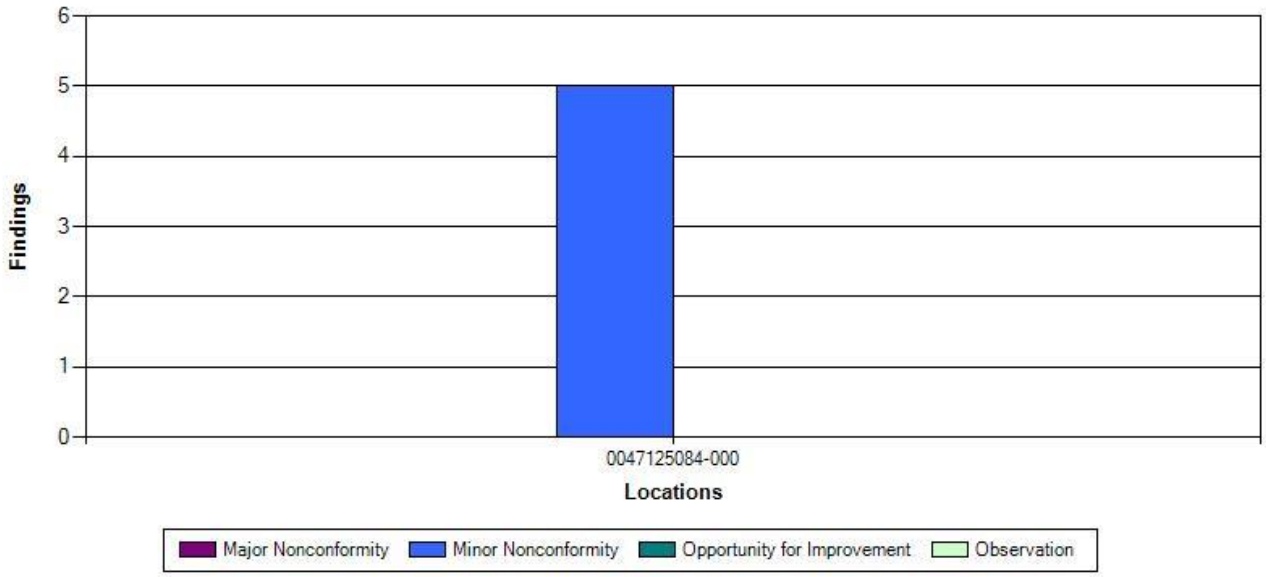
ISO 27001:2013
Health & Care Professions Council management system documentation

NCR Summary

Which standard(s) BSI recorded findings against



Where BSI recorded findings



Definitions:

Nonconformity
Non-fulfilment of a requirement.

Major nonconformity
Nonconformity that affects the capability of the management system to achieve the intended results.
Nonconformities could be classified as major in the following circumstances:
- If there is a significant doubt that effective process control is in place, or that products or services will meet specified requirements;
- A number of minor nonconformities associated with the same requirement or issue could demonstrate a systemic failure and thus constitute a major nonconformity.

Minor nonconformity
Nonconformity that does not affect the capability of the management system to achieve the intended results.

Opportunity for improvement
It is a statement of fact made by an assessor during an assessment, and substantiated by objective evidence, referring to a weakness or potential deficiency in a management system which if not improved may lead to nonconformity in the future. We may provide generic information about industrial best practices but no specific solution shall be provided as a part of an opportunity for improvement.

Observation
It is ONLY applicable for those schemes which prohibit the certification body to issue an opportunity for improvement.
It is a statement of fact made by the assessor referring to a weakness or potential deficiency in a management system which, if not improved, may lead to a nonconformity in the future.

Assessment Participants

Name	Position	Opening Meeting	Closing Meeting	Interviewed (processes)
Roy Dunn	Head of Business Process Improvement	X	X	X
Kayleigh Birtwistle	Quality Compliance Auditor	X	X	X
Andy Sabapathee	IT Infrastructure Engineer			X
Rick Welsby	IT Support Manager			X
Hollie Latham	Policy Officer			X
Claire Harkin	Registration Operations Officer			X
Ben Porter	Education Manager			X
Aveen Croash	Systems & Quality Officer			X
Paula Lescott				X

Outstanding actions from the previous assessment

Ref	Area/Process	Clause
1325464N1	Operations Security (IT Department)	A12.4.3
Scope	IS 600771	
Category	Minor	
Details:	No evidence on how information logs are protected from possible unauthorised changes	
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.	
Cause	Resource to effectively manage logs securely was not in place	
Correction / containment	Process was reviewed and a tool was sourced	
Corrective action	New policy has been created to ensure that logs are protected as required. Admin logs are now protected and access controlled using TripWire. Domain administrators do not have access to the TripWire server, however access is restricted to local administrator accounts. Maintenance and other legitimate access to the account would only be granted by the Head of Business Process Improvement. Passwords are managed using "Password Manager Pro (PMP)" software. Passwords to server restricted to admin for only 2 hours and changed automatically after 30 mins once used. Document reviewed: 1. DOC A12.4.3 Administrator & Operator Logs v1.0 dated 07/04/2017 2. REC MS_4A Improvement Log v1.4	
Closed?:	Yes	

Assessment Findings

The assessment was conducted on behalf of BSI by

Name	Position
Kwadwo Anim-Appiah	Team leader

Assessment conclusion and recommendation

The audit objectives have been achieved and the certificate scope remains appropriate. The audit team 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 continues to achieve its intended outcomes.

RECOMMENDED - The audited organization can be recommended for continued certification to the above listed standards, and has been found in general compliance with the audit criteria as stated in the above-mentioned audit plan.

Use of certification documents, mark / logo or report

The use of the BSI certification documents and mark / logo is effectively controlled.

Findings

Opening Meeting:

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 organisation were also briefed on recent BSI audit delivery and reporting changes, including changes in terminology and executive summary reporting.

Review of Previous Report / NC Closeout / Scope :

Outstanding Minor Non-Conformity (NC) was reviewed and closed out successfully. Please refer to the relevant section for further details.

Scope was confirmed as follows:
"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."

Performance Monitoring & Measurement / ISMS Objectives / Compliance: 6.2, 9.1, A.18:

- Awareness training modules are now released in chunks on monthly basis
- It was noted that objectives have been met and HCPC has set itself same targets for the coming year
- Status of effectiveness measures were seen to have been presented to the Executive Team
- No changes were noted with regards to compliance requirements, however GDPR requirements were seen to have been reviewed and will be presented to the EMT

Planned activities have been fully realised. Planned results achieved.

Document reviewed:
1. HCPC Course Status dated 11/04/2017
2. Six Monthly Information Security Report - dated 27/02/2017
3. DOC A3 Effectiveness Measures v1.3 dated 21/03/2017
4. REC A3 Effectiveness Measures v1.3 dated 23/03/2017
5. GDPR Draft Paper For EMT dated 06/04/2017
6. GDPR Table
7. REC 18 List of Legislation and Regulation v2.2

Internal Audit; Management Review; Corrective Action: 9.2, 9.3, 10:

- Internal audit schedule seen to be well maintained
- Last audit was carried out in March 2017 by ITG on behalf of HCPC
- Audit report from ITG had defined audit scope and criteria as required by the standard
- Audit report was received on 9th April 2017, however the findings raised are being queried by HCPC
- Improvement log (corrective action log) sighted was well maintained
- Findings captured had root causes determined, risk assessed and subsequent actions captured as required
- Executive Management Team (EMT) reviews improvement log on 6 monthly basis
- A supplier audit has been carried out which is commendable
- Management reviews are conducted as part of EMT meetings on monthly basis
- Meeting minutes and agenda reviewed met requirements of the standard
- Six Monthly Information Security Reports are also submitted to the EMT for review

Planned activities have been fully realised. Planned results achieved.

Document reviewed:
1. Internal Audit Report Lead Sheet (13032017) - 13th/14th March 2017
2. REC MS2 Internal Audit Report - Xerox Third Party Suppliers - Sept 2016
3. REC MS_4A Improvement Log v1.4
4. Management Review Procedure QMS
5. Monthly Executive Management Team Meeting - 28/02/2017
6. Six Monthly Information Security Report - dated 27/02/2017

Risk Assessment / Risk Treatment & SOA / Asset Management: 6, 8, A.8:

- Risks are reviewed as part of monthly EMT meetings
-Top 10 risks noted showed only 1 High Risk which was related interruption of electricity supply
- Risk score applied considers impact and likelihood matrix
- Risk levels and risk owners have been identified as required
- No clear mappings of Annex A controls applied to identified risks were sighted

Sampled risks:
2.7 - Interruption to electricity supply
2.11 - Basement flooding
1.5 - Loss of reputation
17.9 - Loss of ISO 27001:2013 certification

- SOA reviewed was at version 1.4 dated 20/03/2017
- SOA reviewed met the requirements of clause 6.1.3d of the standard
- It was commendable to note that CMMI has been considered to determine implementation status of controls
- No exclusions were noted. Reasons for selection were clearly stated within the SOA reviewed

- Information asset inventory is maintained within VsRisk
- Assets have been risk assessed against impact loss of CIA and control referenced as required
- Information Classification and Handling Policy reviewed was appropriate showing required levels: Confidential, Unrestricted, Sensitive and Highly Confidential

Planned activities have been fully realised. Planned results achieved.

Document reviewed:
1. Risk Register and Risk Treatment Plan dated 06/02/2017
2. Statement of Applicability v1.4 dated 20/03/2017
3. DOC A8.1 Asset management v1.3 dated 23/03/2017
4. DOC A8.2 Information Classification and Handling Policy v1.3 dated 23/03/2017

Supplier Relationships / Incident Management: A.15, A.16:
- Key suppliers register maintained with contract agreements attached within Lotus Notes
- Security requirements were seen to have been considered in the agreements sampled
- Business impact assessment seen to have been carried out as required
- Supplier audits have been carried out and reports well maintained
- Incidents are logged within HCPC's improvement log
- Similarly, a separate folder is maintained for Information Incident Report Forms
- A total of 67 information security incidents have recorded since April 2016
- Incidents sampled were seen to have been dealt with and risk assessed as required
- Information security incidents are assessed by the Information Governance Manager

Sampled incidents:
- IIR10.2017 (unredacted bundles)
- IIR15.2017 (Unredacted version had name of victim and her relationship to registrant)
- IIR18.2017 (Unredacted information)

Planned activities have been fully realised. Planned results achieved.

Document reviewed:
1. IIR10.2017 Information Incident Report Form dated 20/03/2016
2. IIR15.2017 Information Incident Report Form dated 29/03/2016
3. HCPC and Xerox Framework Agreement dated 11/04/2015
4. HCPC and Kingsley Napey LLP Agreement 2014
5. REC MS2 Internal Audit Report - Xerox Third Party Suppliers - Sept 2016
6. REC MS2 Internal Audit Report - Archive dated 05/05/2016

Business Continuity: A.17:

- BCP remains appropriate and was last reviewed on 28/02/2017
- Shadow Planner & "Plan In Your Pocket" have been updated to include default test frequency
- "Plan In Your Pocket" sits on encrypted android O/S being trialled iOS
- Two tests have been carried out since the last assessment visit
- Test results sighted were comprehensive inclusive of actions. Test scenarios noted were appropriate

Planned activities have been fully realised. Planned results achieved.

Document reviewed:
1. DOC A.17 Business Continuity Management v1.4 dated 28/02/2017
2. REC MS2 Internal Audit Report - BCM Nov 2016 - Final
3. REC MS2 Internal Audit Report - Registration BCM Test Feb 2017

Physical & Environmental Security: A.11:

- No major changes were noted to physical and environmental security with the exception of the below:
- Major renovations are being undertaken on 186 Kennington Park Road building next to the main office (184)
- Physical and environmental security document have been updated with the major renovation
- Tidy desk policy seen to be adhered to
- Server room was neat with tidy cabling
- Server room was well air-conditioned and had clearly labelled assets

Planned activities have been fully realised. Planned results achieved.

Document reviewed:
1. DOC A.11 Physical and Environmental Security v1.3 dated 17/03/2017
2. DOC A.11.1.5svrrm Working in Secure Areas - Server Room v1.0 dated 09/03/2017

Access Control & Cryptography / Communications Security / System Acquisition, Development and Maintenance: A.9, A.10, A.14:

- Access control policy is in place as documented information
- Access to networks are controlled
- Access provisioning and password management process in place
- Access rights reviews carried out had not been regular
- Passwords and cryptographic keys are managed using "Password Manager Pro" (PMP)
- Privilege accounts are well managed and controlled
- Admin logs are monitored and protected using TripWire and managed by key personnel
- Unique admin credentials are in use which is commendable
- Segregated networks being implemented: Guest VLAN, Building Control, User VLAN, Management VLAN and Server VLAN
- Laptops/Desktops are encrypted using Bitlocker
- Information transferred within the business deemed sensitive or confidential is encrypted using AES 256
- Data is also encrypted at rest with minimum AES 256 standard
- Cryptographic and key management policy was reviewed.
- NDAs are in place and further captured as part of supplier agreements as sighted in earlier sessions
- Network schematics made available were comprehensive showing DMZs, Firewalls, Data VPLS (managed by Exponential-e)
- Sampled change : #20170053 - Dynamic CRM Dev Environment (this was seen to be well controlled as

required).
- Remote access require 2FA via VPN
- Test data is protected as required
- Secure engineering principles such as hardening guidelines for servers was available as documented information
- Annual Pen Test was carried out on HCPC's External Infrastructure Assessment and Web Application Assessment by 3rd party NCC Group.
- Annual Pen Test results reviewed showed 1 High Risk (Outdated Oracle Glassfish Install), 1 Medium Risk (Reflected Cross Site Scripting) and 20 Low Risks (including Detactable Windows Short (8.3) Filenames)
- Above findings have been resolved.

Planned activities and results have not been fully realised/achieved.

Document reviewed:
1. DOC A9.1 Access Control Policy v1.3 dated 17/03/2017
2. DOC A9.2 Access Control Process v1.3 dated 17/03/2017
3. REC A13.1.3 Segregation In Networks v1.1 dated 17/03/2017
4. DOC A13 Communications Security v1.3 dated 23/03/2017
5. Managing Contracts
6. WAN Network Diagram - Exponential-e HCPC Financial Network Designs v2.3 dated 17/03/2017
7. HCPC Gamma Network Diagram
8. Request For Change Form (20170053)
9. DOC A10 Cryptography Policy
10. Annual Penetration Testing - July 2016
11. Internal Infrastructure Penetration Test - March 2017
12. Hardening Guidelines v1.0 dated 13/04/2017
13. Penetration Testing Highlight Report - August 2016
14. Monthly Executive Management Team Meeting - 27/09/2016

Awareness Sampling: Education Team / Policy & Standards / Project :

Education Team (3 staff members interviewed)
Staff interviewed were able to demonstrate knowledge of the below:
- Secure printing
- Information classification requirements
- Confidential emails sent with clear statement that email is confidential
- Posts sent securely as registered mail
- Secure destruction of information
- Staff interviewed had undertaken information security awareness training
- Information security incident reporting requirements
- Location of ISMS related policies
- Tidy desk policy
- Redaction of PII
- Document management control
- Encryption of data

Policy & Standards Team (1 staff member interviewed)
Team is responsible for the following:
- Dealing with enquiries from registered practitioners
- Oversees consultations on documentation
- Receives public input on documentation

- Redaction of PII before publication
- Audience for reports produced were noted as follows: Practitioners, Education Providers, Professional, Members of the public etc
- Internal checks carried out also by the legal team, committee, council and the legal team again before final publication

Knowledge on the following were demonstrated:
- Information security classification requirements
- Information security incident reporting requirements
- Document management control requirements
- Password management

Projects

No member of the team was available for interview on the day of the assessment. The team will be assessed at the next visit.

Planned activities have been fully realised. Planned results achieved.

Document reviewed:
1. Consultation on Revised Standards of Proficiency for Social Workers in England
2. Information Security Policy
3. User Summary Tracker dated 26/01/2017
4. Access Rights - Education dated March 2017
5. Netregulate Job Roles vs Actions v2.0
6. NetReg users & Roles - March 2017

Closing:

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.

Minor (5) nonconformities arising from this assessment.

Ref. no	1465092-201704-N1
Area/Process	Performance Monitoring & Measurement / ISMS Objectives / Compliance: 6.2, 9.1, A.18
Clause	A18.1.1
Scope	IS 600771
Category	Minor
Statement of non conformance:	Legal and regulatory requirements not kept up to date
Clause requirements	Identification of applicable legislation and contractual requirements All relevant legislative statutory, regulatory, contractual requirements and the organization's approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and the organization.
Objective evidence	REC 18 List of Legislation and Regulation v2.2 containing HCPC's legal and regulatory requirements was reviewed and it was noted that majority of the requirements were last reviewed in 2015.
Cause	
Correction / containment	

Ref. no	1465092-201704-N2
Area/Process	Risk Assessment / Risk Treatment & SOA / Asset Management: 6, 8, A.8
Clause	6.1.3
Scope	IS 600771
Category	Minor
Statement of non conformance:	Annex A controls not mapped to identified risks
Clause requirements	Information security risk treatment The organization shall define and apply an information security risk treatment process to: a) select appropriate information security risk treatment options, taking account of the risk assessment results; b) determine all controls that are necessary to implement the information security risk treatment option(s) chosen; NOTE Organizations can design controls as required, or identify them from any source. c) compare the controls determined in 6.1.3 b) above with those in Annex A and verify that no necessary controls have been omitted;

	NOTE 1 Annex A contains a comprehensive list of control objectives and controls. Users of this International Standard are directed to Annex A to ensure that no necessary controls are overlooked. NOTE 2 Control objectives are implicitly included in the controls chosen. The control objectives and controls listed in Annex A are not exhaustive and additional control objectives and controls may be needed. d) produce a Statement of Applicability that contains: • the necessary controls (see 6.1.3 b) and c)); • justification for their inclusion; • whether the necessary controls are implemented or not; and • the justification for excluding any of the Annex A controls. e) formulate an information security risk treatment plan; and f) obtain risk owners' approval of the information security risk treatment plan and acceptance of the residual information security risks. The organization shall retain documented information about the information security risk treatment process. NOTE The information security risk assessment and treatment process in this International Standard aligns with the principles and generic guidelines provided in ISO 31000[5
Objective evidence	Risk Register and Risk Treatment Plan reviewed did not show how Annex A Controls have been mapped to identified risks. The register did not show what controls have been applied in treating the identified risks.
Cause	
Correction / containment	

Ref. no	1465092-201704-N3
Area/Process	Access Control & Cryptography / Communications Security / System Acquisition, Development and Maintenance: A.9, A.10, A.14
Clause	A9.2.5
Scope	IS 600771
Category	Minor
Statement of non conformance:	Review of user access rights requirements not conducted regularly
Clause requirements	Review of user access rights Asset owners shall review users' access rights at regular intervals.
Objective evidence	Access rights review for some of the teams were seen to have been conducted. However, it was noted for example that users with access to NetReg (a critical system) who had left the HCPC still had active accounts. This was so because HCPC had failed to conduct access rights review on a regular basis. Even though the report on users with access to NetReg was sent to the system owner a few weeks ago, the risk associated with having leavers with active accounts had not been considered as required.

	Documents reviewed: 1. Netregulate Job Roles vs Actions v2.0 2. NetReg users & Roles - March 2017
Cause	
Correction / containment	

Ref. no	1465092-201704-N4
Area/Process	Access Control & Cryptography / Communications Security / System Acquisition, Development and Maintenance: A.9, A.10, A.14
Clause	10.1
Scope	IS 600771
Category	Minor
Statement of non conformance:	Findings and subsequent actions from pen test not captured
Clause 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 had failed to capture findings from the pen test report into its improvement log (corrective action log) or even risk assessed internally using its own risk criteria. Similarly, subsequent actions taken was not available as documented information as required by the standard.
Cause	
Correction / containment	

Ref. no	1465092-201704-N5
Area/Process	Access Control & Cryptography / Communications Security / System Acquisition, Development and Maintenance: A.9, A.10, A.14
Clause	6.1.3
Scope	IS 600771
Category	Minor
Statement of non conformance:	Annex A controls wrongly included
Clause requirements	Information security risk treatment The organization shall define and apply an information security risk treatment process to: a) select appropriate information security risk treatment options, taking account of the risk assessment results; b) determine all controls that are necessary to implement the information security risk treatment option(s) chosen; NOTE Organizations can design controls as required, or identify them from any source. c) compare the controls determined in 6.1.3 b) above with those in Annex A and verify that no necessary controls have been omitted; NOTE 1 Annex A contains a comprehensive list of control objectives and controls. Users of this International Standard are directed to Annex A to ensure that no necessary controls are overlooked. NOTE 2 Control objectives are implicitly included in the controls chosen. The control objectives and controls listed in Annex A are not exhaustive and additional control objectives and controls may be needed. d) produce a Statement of Applicability that contains: • the necessary controls (see 6.1.3 b) and c)); • justification for their inclusion; • whether the necessary controls are implemented or not; and • the justification for excluding any of the Annex A controls. e) formulate an information security risk treatment plan; and f) obtain risk owners' approval of the information security risk treatment plan and acceptance of the residual information security risks. The organization shall retain documented information about the information security risk treatment process. NOTE The information security risk assessment and treatment process in this International Standard aligns with the principles and generic guidelines provided in ISO 31000[5
Objective evidence	During the session on "System Development", it was noted that HCPC does not undertake in development in-house and yet the following Annex A Controls had been stated as applicable within the SOA reviewed: A.9.4.5, A.14.2.2, A.14.2.6 and A.14.2.8. It was clear that the above controls had been wrongly included within HCPC's SOA and as such reasons for selection were could not be accepted as required by the standard.
Cause	

Correction / containment	

Our next steps

Next Visit Plan

Date	Auditor	Time	Area/Process	Clause
			DAY 1	
16/04/2018	Eva Arfara	09:00	Opening Meeting / Changes to management system	
		09:30	Top Management: leadership and commitment, context of the organisation, objectives and targets, and ISMS performance improvement	5, A.5
		10:15	Review previous report, confirm status of ISMS and scope	
		10:30	Context of the organisation: internal/external issues and interested parties	4
		11:00	Legislation and compliance	A.18
		11:15	Risk management, and statement of applicability	6, 8,
		12:00	Asset management	A.8
		12:45	**Lunch**	
		13:30	ISMS policy and procedures, internal audits, corrective action	5, 9, 10,
		14:30	Management Review and monitoring of effectiveness of ISMS	
		15:30	Report writing (off site)	
			DAY 2	
Date	**Auditor**	**Time**	**Area/Process**	**Clause**
17/04/2018	Eva Arfara	09:00	Interim meeting	
		09:15	Human Resource Security / Resource Planning	7, A.7
		10:15	Access Control & Cryptography	A.9, A.10
		11:00	Operations Security	A.12

		12:00	Communications Security	A.13
		12:45	**Lunch**	
		13:30	System acquisition, development and maintenance	A.14
		14:30	HR (security awareness sampling)	A.7.2.2
		15:00	IT (security awareness sampling)	A.7.2.2
		15:30	Report writing (off site)	
			DAY 3	
Date	**Auditor**	**Time**	**Area/Process**	**Clause**
18/04/2018	Eva Arfara	09:00	Arrival	
		09:15	Finance Team	
		10:00	Project Management Team	
		10:45	Communications Team	
		11:30	Education Team	
		12:15	Facilities	
		12:45	**Lunch**	
		13:30	Secretariat & Customer Services	
		14:15	Policy & Standards	
		15:00	Fitness to Practise	
		16:00	Report writing (off site)	
			DAY 4	
Date	**Auditor**	**Time**	**Area/Process**	**Clause**
19/04/2018	Eva Arfara	09:00	Arrival	
		09:15	Registrations	
		10:15	Physical & Environmental Security	A.11
		11:15	Business Continuity	A.17
		12:00	Security Incident Management	A.16
		12:45	Lunch	
		13:30	Supplier Relationships	A.15
		14:30	Follow up on audit trails	
		15:15	Update of 3-year plan and agree dates for next visit	
		16:00	Closing meeting	

			DAY 5	
Date	**Auditor**	**Time**	**Area/Process**	**Clause**
20/05/2018	Eva Arfara	09:00	Report write-up offsite as agreed with client	
		12:30		

Next visit objectives, scope and criteria

The objective of the assessment is to conduct a re-assessment of the existing certification to ensure the elements of the proposed scope of registration and the requirements of the management standard are effectively addressed by the organisation's 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.

ISO 27001:2013
Health & Care Professions Council management system documentation

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.

Your next steps

NCR close out process

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

5 minor nonconformities requiring attention were identified. These, along with other findings, are 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.

How to contact customer service

'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).

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

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

Tel: +44 (0)345 080 9000

Email: MK.Customerservices@bsigroup.com

Appendix: Your certification structure & on-going assessment programme

Scope of Certification

IS 600771 (ISO/IEC 27001:2013)

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 1.4 dated 20/03/2017.

Assessed location(s)

The audit has been performed at Central Office.

London / IS 600771 (ISO/IEC 27001:2013)

Location reference	0047125084-000
Address	Health & Care Professions Council Park House 184 Kennington Park Road London SE11 4BU United Kingdom
Visit type	Continuing assessment (surveillance)
Assessment reference	8495236
Assessment dates	12/04/2017
Deviation from Audit Plan	No
No. of Full Time Equivalent Employees	250
Total No. of Effective Employees at the site	250
Scope of activities at the site	Main Certificate Scope applies.
Assessment duration	2 day(s)

Changes in the organization since last assessment

The following changes in relation to organization structure and key personnel involved in the certified management system were noted:

Fitness & Practice department now have sub-teams specialising in Assurance, Operations and Development. each process handled.

The following changes in relation to the certified organization activities, products or services covered by the scope of certification were identified:

Social Workers who are a third of HCPC's register would be moved to a new regulator potentially.

There was no change to the reference or normative documents which is related to the scope of certification.

Certification assessment programme

Certificate Number - IS 600771

Location reference - 0047125084-000

		Audit1	Audit2	Audit3	Audit4	Audit5	Audit6
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

Notes

This report and related documents are 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. 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.

This audit was conducted on-site through document reviews, interviews and observation of activities. The audit method used was based on sampling the organization's activities and it was aimed to evaluate the fulfilment of the audited requirements of the relevant management system standard or other normative document and confirm the conformity and effectiveness of the management system and its continued relevance and applicability for the scope of certification.

As this audit was based on a sample of the organization's activities, the findings reported do not imply to include all issues within the system.

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.