Audit Committee 12th June 2018

BSI ISO27001 audit

Executive summary and recommendations

Introduction

BSI have been on site to carry out the ISO27001 recertification audit. This was a 4 day audit on site, plus 1 ½ days offsite preparation and report writing. Kayleigh Birtwistle stood in for Roy Dunn on the first day of audit, and coped well with the challenge.

The audit had been delayed by BSI due to lack of resource. The audit took place in the third week of the new HCPC Management Structure.

- HCPC have been recommended for recertification.
- Three non conformances were identified;
- a) some improvement log entries were closed but data was incomplete (root cause),
- b) the ISMS documentation was updated in “draft status” reflecting the new HCPC Management Structure, rather than being incorrect but signed off
- c) Mail sacks were left in the Reception area for collection, and were insecure.
- Three opportunities for improvement were highlighted;
- i) the HR key safe pin code had not been changed in a year and could be known by departed employees
- ii) the business continuity plan had not been tested in a year, we were waiting to complete the relocation of our primary DR site from Uxbridge to Wapping, and the change to HCPC Management structure,
- iii) specific clauses on information security should be added to the Relationship Manager responsibilities.

Decision

The Audit Committee are asked to note the report.

Resource implications

None known

Appendices

BSI Audit report ISO27001:2013 – May 2018

Date of paper

4th June 2018

Assessment Report

Health & Care Professions Council

Assessment dates	21/05/2018 to 25/05/2018 (Please refer to Appendix for details)
Assessment Location(s)	London (000)
Report author	Simon Evans
Assessment Standard(s)	ISO/IEC 27001:2013

Table of contents

Executive summary 4
Changes in the organization since last assessment 4
NCR summary graphs 5
Your next steps 5
NCR close out process 5
Assessment objective, scope and criteria 6
Assessment participants 7
Assessment conclusion 8
Findings from previous assessments 9
Findings from this assessment 12
Opening Meeting / Changes to management system: 12
Top Management: leadership and commitment, context of the organisation, objectives and targets, and ISMS performance improvement. 5, A.5: 12
Review previous report, confirm status of ISMS and scope: 12
Context of the organisation: internal/external issues and interested parties. 4: 13
Legislation and compliance. A.18: 13
Risk Management, and Statement of Applicability. 6, 8: 14
Asset Management. A.8: 15
ISMS policy and procedures, internal audits, corrective action. 5, 7, 9,10: 15
Management Review and monitoring of effectiveness of ISMS: 16
Human Resource Security / Resource Planning. 7, A.7: 17
Access Control & Cryptography. A.9. A.10: 18
Operations Security. A.12: 19
Communications Security. A.13: 20
System acquisition, development and maintenance. A.14: 21
Security Awareness A.7.2.2: 21
Physical & Environmental Security A.11: 24
Business Continuity A.17: 25
Security Incident Management A.16: 26
Supplier Relationships A.15: 26
Update of 3-year plan and agree dates for next visit: 27

Minor (3) nonconformities arising from this assessment.....28
Next visit objectives, scope and criteria.....30
Next visit plan.....31
Appendix: Your certification structure & on-going assessment programme.....32
Scope of certification.....32
Assessed location(s).....32
Certification assessment programme.....33
Mandatory requirements – recertification.....34
Definitions of findings:.....35
How to contact BSI.....36
Notes.....36
Regulatory compliance.....37

Executive summary

In line with the strategic direction of the organisation and the intended results of the Information Security Management System, particularly with regard to the areas assessed at this recertification visit, it was identified that the management system has demonstrated it is designed to support the strategic direction and delivers the intended results.

The organization was noted to be continuing to maintain and improve the processes effectively with particular regard to the following areas:
- Excellent starter signed documentation covering all aspects of IS policies and requirements prior to the start date
- Education and awareness of staff
- IS consideration in project management

However, there are further possible Opportunities for Improvement which will reduce risk and assist with achieving the intended result:
- Closure and evaluation of NCRs
- Publishing of draft documents

All audit participants are thanked for their assistance in enabling the audit to run smoothly and to schedule

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:

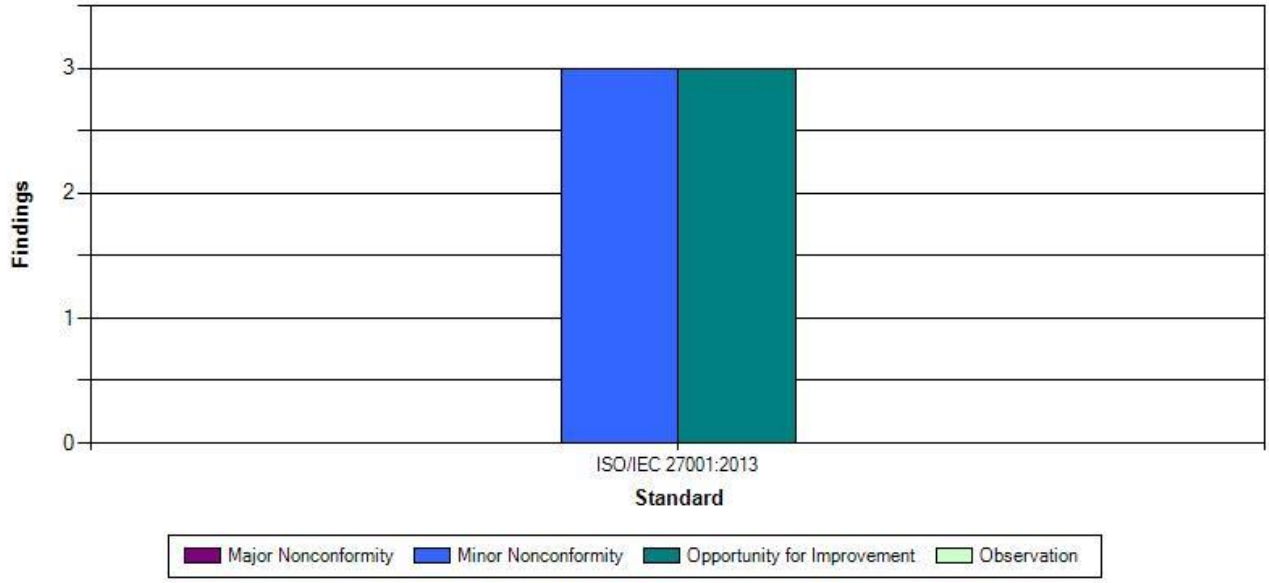
Executive management team was streamlined from nine to three executive directors; taking effect from 07/05/2018. This has allowed a consolidation of departments from a managerial perspective; however there has not been a significant change in the overall head count.

No change in relation to the audited organization's activities, products or services covered by the scope of certification was identified.

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

NCR summary graphs

Which standard(s) BSI recorded findings against



Your next steps

NCR close out process

Corrective actions with respect to nonconformities raised at the last assessment have been reviewed. Actions were not found to be effectively implemented in all areas. Such areas, identified in subsequent sections of the report, will be further reviewed for closure at the next assessment.

3 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.

Please refer to Assessment Conclusion and Recommendation section for the required submission and the defined timeline.

Assessment objective, scope and criteria

The objective of the assessment was to conduct a reassessment 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 organization's management system.

If this visit is part of a multi-location assessment, the final recommendation will be contingent on the findings from all assessments.

The scope of the assessment is the documented management system with relation to the requirements of ISO27001 and the defined assessment plan provided in terms of locations and areas of the system and organization to be assessed.

The criteria of the assessment are BS EN ISO27001:27001 in relation to Health and Care Professions Council management system documentation.

Assessment participants

Name	Position	Opening meeting	Closing meeting	Interviewed (processes)
Kayleigh Birtwistle	Quality Compliance Auditor	X	X	X
Marc Seale	Chief Executive and Registrar			X
Jaqueline Ladds	Executive Director of Policy and External Relations			X
Rick Welsby	IT Support Manager			X
Elandre Potgieter	Senior Service Support Analyst			X
Andy Sabapathee	Infrastructure Engineer			X
Tim Kitchener	Senior project Manager			X
Roy Dunn	Head of Business Process Improvement		X	X
Jagana Abubacarr	Finance Officer			X
Zoe Yankson	Purchase ledger officer			X
Sam Ha	HR Advisor			X
Layanta Palmer	HR Advisor			X
Daniel Knight	Publishing Manager			X
Natalie Osei-Owusu	Events Officer			X
Jamie Hunt	Education Manager			X
Robert Pope	Facilities Manager			X
Giba Rahman	Governance and appointments officer / EA			X
Rebecca Bryan	Quality Compliance Manager			X
Siobhan Carson	Case Manager			X
Katherine Timms	Acting Director of Policy and Standards			X
Andrew John	Acting Registration Manager			X
Sammuel Yemane	Registration Manager			X
Andrew Powell	Facilities Officer			X
Jason Roth	IT Infrastructure Manager			X

Assessment conclusion

BSI assessment team

Name	Position
Simon Evans	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 the organization 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 - Corrective Action Plan Required ('Minor' findings only): The audited organization may be recommended for continued certification, based upon the acceptance of a satisfactory corrective action plan for all 'Minor' findings as shown in this report. Effective implementation of corrective actions will be reviewed during the next surveillance audit.

Please submit a plan to BSI detailing the nonconformity, the cause, correction and your proposed corrective action, with responsibilities and timescales allocated. The plan is to be submitted no later than **01/06/2018** by e-mail to msuk.caps@bsigroup.com, referencing the report number, or through the BSI Assurance Portal if this is enabled for your account.

Use of certification documents, mark / logo or report

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

Findings from previous assessments

Finding Reference	1465092-201704-N1	**Certificate Reference**	IS 600771
Certificate Standard	ISO/IEC 27001:2013	**Clause**	A18.1.1
Category	Minor		
Area/process:	Performance Monitoring & Measurement / ISMS Objectives / Compliance: 6.2, 9.1, A.18		
Details:	Legal and regulatory requirements not kept up to date		
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	Incorrect version had been saved to the company ISMS as a document control error		
Correction / containment	Correct version was subsequently uploaded. Revision REC18.1A 0050728/0004 dated 08/02/2018		
Corrective action	Physical checks are now in place following system restores to ensure all current documents have carried forward as part of the restore		
Closed?:	Yes		

Finding Reference	1465092-201704-N2	**Certificate Reference**	IS 600771
Certificate Standard	ISO/IEC 27001:2013	**Clause**	6.1.3
Category	Minor		
Area/process:	Risk Assessment / Risk Treatment & SOA / Asset Management: 6, 8, A.8		
Details:	Annex A controls not mapped to identified risks		
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	Improvement of understanding of the standard and requirements		
Correction / containment	SoA reviewed		
Corrective action	SoA amended and reviewed annually and subject to internal audit for validity and linked to risks		
Closed?:	Yes		

Finding Reference	1465092-201704-N3	**Certificate Reference**	IS 600771
Certificate Standard	ISO/IEC 27001:2013	**Clause**	A9.2.5
Category	Minor		
Area/process:	Access Control & Cryptography / Communications Security / System Acquisition, Development and Maintenance: A.9, A.10, A.14		
Details:	Review of user access rights requirements not conducted regularly		
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	No process in place		
Correction / containment	There was no immediate corrective action taken to carry out an meditate check of access control rights		
Corrective action	A list is now sent to all managers listing users and levels of access. The response back from managers has been slow, and some have not responded, which was highlighted in an internal audit by IT Governance		
Closed?:	No		
Justification	See NCR 630565-201805-N2 to this report		

Finding Reference	1465092-201704-N4	**Certificate Reference**	IS 600771
Certificate Standard	ISO/IEC 27001:2013	**Clause**	10.1
Category	Minor		
Area/process:	Access Control & Cryptography / Communications Security / System Acquisition, Development and Maintenance: A.9, A.10, A.14		
Details:	Findings and subsequent actions from pen test not captured		
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 action taken was not available as documented information as required by the standard.		
Cause	Pen test vulnerabilities are internally graded as Highly Confidential and had not been shared with the BI team for the audit		
Correction /	Pen test reports and trackers are maintained the IT Director		

containment	
Corrective action	IT now keeping a full tracker (observed) to follow through on remediation actions
Closed?:	Yes

Finding Reference	1465092-201704-N5	**Certificate Reference**	IS 600771
Certificate Standard	ISO/IEC 27001:2013	**Clause**	6.1.3
Category	Minor		
Area/process:	Access Control & Cryptography / Communications Security / System Acquisition, Development and Maintenance: A.9, A.10, A.14		
Details:	Annex A controls wrongly included		
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	Better understanding of internal v external development responsibilities		
Correction / containment	SoA reviewed and controls removed		
Corrective action	Annual review of SoA which is then subject to internal and external audit		
Closed?:	Yes		

Findings from this assessment

Opening Meeting / Changes to management system:

The formal opening meeting included the objective of the assessment, methodology and terminology used, confidentiality, number of staff in scope, purchase order details, and the agreed assessment plan.

There has been no significant change to the ISMS

Top Management: leadership and commitment, context of the organisation, objectives and targets, and ISMS performance improvement. 5, A.5:

The Chief Executive and Executive Director of Policy and External Relations were interviewed. They demonstrated key strategic direction of the organization and fully understood the risks carried.

Executive management team was streamlined from nine to three executive directors; taking effect from 07/05/2018. This has allowed a consolidation of departments from a managerial perspective; however there has not been a significant change in the overall head count.

The restructuring of the organization's Senior Leadership was discussed. This allows the flexibility for the business to grow in line with its strategic direction.

Key risks included:
- Cyber attack
- Loss of registrant details

It was clear that there are regular meetings, and reporting mechanisms, in place to keep the Senior Leadership up to date with security strategy and the ability to clearly drive, from Senior Leadership down, a business culture which reflects the organizations IS requirements and those of its registrants.

Effectiveness: The good objective evidence gathered in this section identified that Top Management are involved within IS and are providing key strategic direction of how they wish the culture to be deployed across the organization

Review previous report, confirm status of ISMS and scope:

The previous report was viewed and the NCRs raised were discussed. Four NCRs were closed and one remains open.

The organizations ISMS is still deemed to be fully effective within the business and is fully documented.

There has a revision update to the scope; however, the context has not changed:

> Scope statement: The management of 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 SoA v1.7 dated 16/05/2018.

Context of the organisation: internal/external issues and interested parties. 4:

The context of the organization is fully understood internally and documented in the ISMS Manual :

ISMS Manual, v2 dated 02/05/2018 was viewed
- A full list of interested parties, the needs and expectations of internal parties has been captured at Para 3

External interested parties included:
- Applicants and registrants
- ICO
- Regulatory bodies
- Members of the public
- Professional services
- Consultants
- Local Authority
- Business Clients

Internal Interested parties include:
- Employees and contractors (including partners)
- Council members

Effectiveness: The good objective evidence gathered in this section identified that planned objectives have been realised and planned results have been achieved

Legislation and compliance. A.18:

Rec 18.1A List of Legislation and Regulation, v2.5 dated 08/02/2018 was viewed
- Document provides a full list of legislative and regulatory Acts
- 43 Acts have been included

A snapshot of those included are:
- Data Protection Act
- Computer Misuse Act
- RIPA
- Health and Social work professions order
- Anti Bribery Act
- H&S at work Act

A third party legal company acts on behalf of the organisation for legislative changes and cases and have reviewed the list of legislation and regulation on 28/03/2018

Effectiveness: The good objective evidence gathered in this section identified that planned objectives have been realised and planned results have been achieved.

Risk Management, and Statement of Applicability. 6, 8:

Risk Management
Doc A2 Risk Management, v1.5 dated 27/03/2018, was viewed
- Top 10 risks noted showed only 1 High Risk which was related interruption of electricity supply
- Document was approved by the Chief Executive at the Executive Management Team
- Full risk analysis methodology is included
- Control matrix will allow consistent, valid and comparable results

Risks Sampled:
- Risk 17.1
- Risk 5.1
- Risk 2.6
- Risk 15.7

Risk 17.1, loss of information from HCPC electronic databases due to inappropriate removal by an employee, was viewed
- The risk was assessed and evaluated in line with the A2 Risk Management Document
- The risk is aligned correctly to Annex A controls

Risk 5.1 Software Malware damage.
- The risk was assessed and evaluated in line with the A2 Risk Management Document
- The risk is aligned correctly to Annex A controls

Risk 2.6 Inability to accommodate HCPC employed
- The risk was assessed and evaluated in line with the A2 Risk Management Document
- The risk is aligned correctly to Annex A controls

Risk 15.7 Card record theft
- The risk was assessed and evaluated in line with the A2 Risk Management Document
- The risk is aligned correctly to Annex A controls

The risks assessed directly track back into the organizations IS Objectives as recorded in the ISMS Policy, v1.4 dated 21/03/2018

A total number of 42 IS risks have been identified on the current risk register

Statement of Applicability
- SoA v1.4 dated 20/03/2017, was viewed and is currently showing as being the last approved SoA
- SoA v1.5 dated 18/04/2017, was viewed in the archive as being Draft with the excluded Annex A controls A9.4.5, A14.2.2, A14.2.6 and A14.2.8 removed following the NCR (1465092-201704-N5) raised during the last CAV
- SoA v1.6 dated 27/03/2018, was viewed in archive as being in Draft XXXX
- SoA v1.7 dated 16/05/2018 was viewed in the ISMS as being in Draft. This document is awaiting authorisation in the next scheduled SMT meeting on 26/06/2018 (See NCR 1630565-201805-N1)
- SoS v1.7 is clear in the justification for inclusion and exclusion and links to additional supporting documentation within the ISMS

Effectiveness: On the whole good objective evidence gathered in this section identified that planned objectives have been realised and planned results have been achieved. However, please note the NCR raised under the ISMS Policies and Procedures section of this report

Asset Management. A.8:

High level Information Asset List, Rec2A dated17/05/2018 was viewed
- Document is provided to the EMT for oversight
- Document is a high level overview of the physical and logical assets held

Microsoft SCCM is in use to fully track IT assets and correlated to users within Active Directory

Desktops are not individually assigned as a hot desk environment is deployed
- Local drives are hidden and no data can be saved to the drive
- Assets PC427 and PC290 were sampled and were located as described

Laptops
- 10 pool laptops are available for staff to use via a booking and signing out system (Viewed)
- Issued laptops are provided to a small number of staff
- The tracking of laptop issue is maintained through SCCM and Active Directory
- Assets LT132, LT140, LT147 were sampled and were correctly assigned, and tracked, in line with process

Servers
- All servers are tracked in VMWare
- Approval for infrastructure equipment goes through CAB process
- Equipment Asset tags are used as the unique identifier

Disposals
- IT Equipment Disposal Document, ISMS Doc 11.2.7.1 was viewed
- Financial approval prior to disposal
- Disposals a conducted by 3rd party; Computer Disposals Ltd
- Disposal certificate J025370 dated 05/10/2017 was viewed
- Certificated showed the disposal 24 HHDs, 11 desktops, 109 mobile phones, 3 laptops, 4 monitors and sundry items

Classification
- Information Classification and Handling Policy DOCA8.2, v1.6 dated 15/05/2018 was viewed
- Four classifications were noted (Unrestricted, Restricted, Confidential and Highly Confidential)
- Classifications are applied to documents: EMP Meeting document, dated 27/06/2-17, was sampled
- Email has the ability to set classification as necessary
- Certain group mailboxes, such as Registrations and Fitness to Practice, have default classifications set

Effectiveness: The good objective evidence gathered in this section identified that planned objectives have been realised and planned results have been achieved

ISMS policy and procedures, internal audits, corrective action. 5, 7, 9, 10:

A full list of ISMS policies, and supporting documents were viewed on the intranet.
- Some documents were noted to still be in draft format even though they are deemed to be published (See NCR)
- All mandated documents required by the standard are included in the ISMS lists
- All documents have been reviewed, even if not all have been authorised, annually
- All documents have version control, are dated and have an owner assigned

Internal Audit and Corrective Actions
- Internal Audit schedule for 2018, v 2.0 dated 03/01/2018, was viewed
- Schedule provides a full internal audit, carried out by IT Governance in 02/2018
- Multiple mini-audits, relating to clear desk, security training, pen test audits were viewed as being scheduled throughout the year.
- Audit report, ITG-7190-HTPC-27001IA dated 07/02/2018 was viewed
- The audit had a scope and context assigned
- Audit was conducted by IT Governance
- 3 NCRs and 15 OFIs were raised during the audit
- 3 NCRs were tracked into the Improvement Log at entries 516-518
- 15 OFIs were tracked into the Improvement Log at entries 519-533
- Internal Audit NCR 1 at Improvement Log entry 516 was fully viewed
- Improvement Log Entry 417 related back into BSI NCR3 regarding access issues and has highlighted, slow or non-returns from individual areas of the business
- Improvement Log Entry 516 (IT Governance NCR1) and Entry 417 (BSI NCR3) are shown in the Improvement Log as being closed but there is no closure date (See NCR to this section)

Effectiveness: With the two Minor Non conformities raised in this section, it is identified that planned objectives have not been fully realised and results have not been fully achieved.

Management Review and monitoring of effectiveness of ISMS:

Management reviews are conducted as part of EMT meetings on a monthly basis. The meetings cover updates and upstanding issues carried over from previous meetings

Changes to internal and external risks are presented for approval or acceptance as they occur
- Minutes from the meetings scheduled were viewed for 25/07/2018 which outlined the risk management acceptance and presentation of the risk register to demonstrate external issues
- Minutes record the acceptance of an approach for a risk management control for a 3rd party supplier

Extracts from the improvement log are presented to the EMT to feedback on performance
- Minutes for the EMT meeting 24/04/2018 were viewed to demonstrate that the improvement log was presented
- All open actions were noted and accepted

Feedback from interested parties is provided back to Information Governance Manager
- GDPR requirements have been the largest feedback recently through external audits

Opportunities for improvement raised in EMT (MR)
- Following the issue of any 'Near Miss Reports' they are then presented to the EMT
- EMT meeting dated 31/10/2017 was observed to have 'Near Miss Report 63' issued
- Subject was regarding Payroll and pay runs
- Full report issues and recommendations in the report with recommendations transferred into the Improvement Log
- Improvement Log entry 421 was observed to show the transfer and tracking of the improvement

Objective setting
- A list of IS objectives was observed as presented to the EMT on 27/02/2018
- The minutes from the above meeting record that the objectives were agreed

Security Incident Review
- Minutes from the EMT meeting on 27/02/2018 documents the review of security incidents

Effectiveness: Whilst there is no specific meeting titled 'Management Review' the mandated elements are included in the monthly EMT meetings throughout the year. The good objective evidence gathered from the EMT meetings identified that planned objectives have been realised and planned results have been achieved

Human Resource Security / Resource Planning. 7, A.7:

Resource Planning and Competence
The Business Improvement staff, with ISMS responsibilities, have demonstrated the following experience and viewed qualifications:
- ISO27001:2013 transition certificate
- Practitioner in Information Security
- Certificate in Information Security Management Principles
- ISO27001:2013 Internal Auditor

Staff have IS considerations logged as part of their individual CPD plans for 2018/19
- Business Continuity and Training
- Risk Management
- Attendance at Certified CISO course
- QA diploma

New Starters
A sample of new starter records were reviewed N C[redacted] (16/04/2018 start date) and L D[redacted] (27/03/2017).
The following records were observed kept:
- Starter Checklist used to ensure that the process has been followed including key polices
- Full right to work checks carried out and documents observed
- Signed Contractual Documents including confidentiality
- Signed data handling guidance document
- Signed Email guidance document
- Signed IT policy document including confidentiality of data, access control, security, passwords, monitoring and unacceptable behaviour
- Induction Training within one week of start
- DBS record for D[redacted] was observed (not all staff require disclosure - only for access to vulnerable adults and children)

Movers/Transfers
- A sample of 2 movers was reviewed (records for staff numbers 584 and 675)
- Transfer is maintained via the core HR system
- Observed records kept showing:
- Role amended
- New contract; including confidentiality
- Weekly HR report captures movers
- Receiving Line manager raises an internal IT request for access changes

Leavers
A sample of records for leavers was observed: S D[redacted](Left 12/03/2018) and B A[redacted] (11/05/2018). The following was observed respectively
- Leaver process has been followed.
- Resignation acceptance letters observed and confirmation of that resignation
- Exit interview only for A[redacted] (these are optional for the staff member)
- Access removed for both staff members was confirmed

Contracts and pre-start documentation observed contained provisions for:
- Confidentiality
- Data Protection
- Intellectual Property
- Their role in IS

Effectiveness: The good objective evidence, especially with the new starter paperwork, gathered in this section identified that planned objectives have been realised and planned results have been achieved.

Finding Reference	1630565-201805-I1	**Certificate Reference**	IS 600771
Certificate Standard	ISO/IEC 27001:2013	**Clause**	A11.1.3
Category	Opportunity for Improvement		
Area/process:	Human Resource Security / Resource Planning. 7, A.7		
Details	Consideration to change the pin code for the key safe at regular intervals should be made. The current combination has not been changed for some time even though staff have left the department. There is still defence in depth around the information being protected hence an OFI and not NCR.		

Access Control & Cryptography. A.9. A.10:

Cryptography
- DOC A10 Cryptography Policy, v1.6 dated16/05/2018 was viewed
- Document provides a list of which systems are encrypted
- Keys are stored in an encrypted key vault in Azure
- All cryptographic keys for publically available information use keys generated from public certificate authority
- Workstation encryption keys are contained in a restricted folder within Active Directory
- Access to keys is strictly controlled to key IT staff
- Legal compliance is considered in the viewed policy

Access control
- IT staff have normal user accounts and then domain, or local admin account, as an addition
- 11 Domain admin accounts were viewed in Active Directory
- Viewed list was fully authorised and up to date
- Domain accounts are only approved via the Security Assurance Board
- S20170002 was sampled to show the approval review process for continuing Domain Account authorisation
- Above request and review were formally agreed following review

- All normal user accounts are unique to the user and have passwords which are complex and changed every 42 days

Starters
- User accounts are created following starter request from HR as a weekly report or individual request
- Account creation for T[redacted] P[redacted] and G[redacted] S[redacted] were sampled
- Starter requests are standardised and were viewed
- Line manager has input into the access levels required
- Ticket 120545 was viewed in relation to T[redacted] P[redacted] with relevant access requirements submitted
- G[redacted] S[redacted] is yet to start therefore a creation ticket is not yet in place

Access review
- Access reviews are conducted monthly with IT sending out a list to managers to confirms users and their access
- Email of users list for 04/04/2018 was sampled
- All expected returns were present and tracked via email copy into a specific folder
- Email responses from the education response and finance were viewed for completeness

Leavers
- HR inform IT of any intended leavers and follows process
- Account for A[redacted] G[redacted] was sampled as he is due to leave the business on 25/05/2018
- Account was viewed to show the expiry date has now been set for the day of leaving
- Account for A[redacted] S[redacted] was sampled
- Account was viewed in AD as being disabled

Effectiveness: The good objective evidence gathered in this section identified that planned objectives have been realised and planned results have been achieved.

Operations Security. A.12:

Change Management
- Weekly CAB is place
- CAB for 10/05/2018 was viewed
- Master change list is maintained and was sampled

Sampled Changes
RFC 21080046 (password length change) was sampled and contains details of requestor, reasons for change, implementation steps, back out plan test requirements, impact on DR, licencing issues and CIA consideration.
- RFC was approved with quorum of staff authorising
- Change was communicated to the business as it impacted every user

RFC 20180043 (DDoS Protection for MS Azure Network) was sampled and contains details of requestor, reasons for change, implementation steps, back out plan test requirements, impact on DR, licencing issues and CIA consideration.
- RFC was approved with quorum of staff authorising

Protection from Malware
- Symantec Endpoint Protection is deployed
- Version 14.[redacted] was viewed as being deployed
- Definition r[redacted] was noted as being deployed

- SCCM is in use to deploy vendor patches to test group and then onto the wider network

Control of Software
- Devices are tied down to prevent upload of unauthorised software (Local Admin only can upload)
- Applocker policies are applied
- Acceptable use policy covers deployment of software

Capacity Management
- Weekly capacity report is produced for weekly internal IT meeting
- Capacity reports dated 13/04/2018 and 14/07/2107 were sampled
- Servers have alarm thresholds set at 95% CPU utilization and 93% disc space utilization
- Samples reports were all within acceptable thresholds

Logging and Monitoring
- Logs are retained in TripWire on RAID 5
- System Logs are reviewed monthly following the patching cycle by IT
- 5 months logs are retained before being overwritten
- Request to release the password for log review is requested to prevent any potential tampering

Backup
- Backup policy v1.2 dated 10/05/2018 was viewed
- Back up to on premise and Cloud based environment
- Backups are encrypted at DB level
- Data is backed up incrementally

Pen Testing
- Internal Pen Test report, conducted by 3rd party provider (CREST Registered)
- Full scope and context included in the test and agreed with the organization in the proposal document
- Test completed by 3rd party conducted in 03/2018
- Report highlighted 10 vulnerabilities (3 high, 3 medium, 3 low and 1 information)
- HCPS-024-1-2 a medium risk was sampled
- Vulnerability was tracked into the Security Advisory Board meeting reference 20180028
- Sampled vulnerability has been closed out following work tracked in the SAB request

Effectiveness: The good objective evidence gathered in this section identified that planned objectives have been realised and planned results have been achieved

Communications Security. A.13:

Information Transfer
- Bitlocker deployed on laptops and desktops
- Data is encrypted prior to transfer
- USBs are encrypted prior to any transfer
- Personal external USBs are not whitelisted for internal data transfer
- Transfer mechanisms are covered in ISMS DOCA10
- Exchange in O365 is covered with Advanced Threat Protection for incoming mail
- DLP is not activated in O365
- Azure Information Protection (including rights management) is a 2018 project

Security of Network Services
- External licencing agreements for the provision of services, such as Microsoft, were viewed

- Firewalls and IDS and IPS are in place for on-site and off-site service
- Agreements with Rackspace were viewed

Segregation of Networks
- Segregation of Networks document REC A13.1.3, v1.2 dated 17/05/2018, was viewed
- Document outlines the name of the network, its segregation, who is allowed access and the type of data stored

Effectiveness: The good objective evidence gathered in this section identified that planned objectives have been realised and planned results have been achieved

System acquisition, development and maintenance. A.14:

All desktops and laptops follow a standardised build within SCCM

There is no internal software development as all development is outsourced with an Internal Project Manager assigned

OWASP Top 10 vulnerabilities are considered as part of the external development program

Live project for new corporate web site was sampled:
- Business case was submitted, dated 04/2016
- Business case approved by EMT
- Project is aligned to Prince 2 methodology
- Phases included initiation with a PIA
- Supplier was used to define the solution which provide the requirements list for functional and non-functional requirements
- Analysis of platforms was conducted
- Requirements log captured security elements at entries SEC01 to SEC34
- Suppliers were benchmarked for compatibility along with security prior to selection
- Security requirements were future proofed; PCI:DSS requirements were added but not yet required
- Full project plan is compiled along with a supplementary project plan by the developer
- Independent pen test is scheduled for the project (not the developer conducting)
- Test data is protected by the developer; test data is performed using publically available data
- UAT performed by organisation with load testing conducted by independent 3rd party
- Current anticipated completion date is 26/10/2018

Effectiveness: The good objective evidence gathered in this section identified that planned objectives have been realised and planned results have been achieved

Security Awareness A.7.2.2:

The organization have implemented a monthly IS training and awareness CBT package broken down into six modules. The modules covered include:
- Module 1 Introduction to IS (97% completion rate)
- Module 2 Scenarios (94% completion rate)
- Module 3 Physical Security (91% completion rate)
- Module 4 Digital Security (87% completion rate)
- Module 5 Information Protection and Incidents (86% completion rate)
- Module 6 Important Documentation Assessment (issued 04/2018 and awaiting completion figures)

HR
2 staff were sampled. Good knowledge was demonstrated in:
- Passwords
- Incident management
- Polices location
- Tidy desk and clear screen
- Data transfer
- Data encryption
- Change controls
- Protection of PII

IT
2 staff were sampled. Good knowledge was demonstrated in:
- Passwords
- Incident management
- Polices location
- Tidy desk and clear screen
- Data transfer
- Data encryption
- Change controls
- Protection of PII
- Training and awareness certificates for the department were displayed on notice board

Finance Team
2 staff were sampled. Good knowledge was demonstrated in:
- Password control
- Incident management
- Polices location
- Tidy desk and clear screen
- Data transfer
- Clock synchronisation and AV updates
- Protection of PII and sensitive finance data
- Training and awareness sessions were viewed

Project Management Team
Single staff member was sampled. Good knowledge was demonstrated in:
- Security policies
- Incident management and reporting
- Signposting policy location
- Tidy desk and clear screen
- Clock synchronisation and AV updates observed
- Training and awareness sessions were viewed

Communications Team
2 staff were sampled. Good knowledge was demonstrated in:
- Password control
- Incident management
- Polices location
- Tidy desk and clear screen
- Data transfer

- Clock synchronisation and AV updates observed
- Data transfer
- Training and awareness sessions were viewed

Education Team
Single staff member was sampled. Good knowledge was demonstrated in:
- Password control
- Incident management
- Polices location
- Tidy desk and clear screen
- Data transfer
- Data classification
- AV updates observed
- Training and awareness sessions were viewed

Facilities (Office Services)
Single staff member was sampled. Good knowledge was demonstrated in:
- Password control
- Incident management
- Polices location
- Tidy desk and clear screen
- Data transfer
- Data classification
- AV updates observed
- Physical security controls
- Training and awareness sessions were viewed

Secretariat
Single staff member was sampled. Good knowledge was demonstrated in:
- Email security
- Password control
- Incident management
- Clock synchronisation and AV updates observed
- Polices location
- Secure data transfer and encryption
- Training and awareness sessions were viewed
- Folder access control viewed and could no see other departments

Policy & Standards
Single staff member was sampled. Good knowledge was demonstrated in:
- Email security
- Password control
- Incident management
- Clock synchronisation and AV updates observed
- Polices location
- Folder access control viewed and could no see other departments

Fitness to Practise
2 staff were sampled. Good knowledge was demonstrated in:
- Protection of data in case management system
- Good password control

- Clock synchronisation and AV updates observed
- Departmental security policies observed
- Corporate IS policies signposted
- Network folder restrictions in place

Registrations
2 staff were sampled. Good knowledge was demonstrated in:
- Good demonstration of incident management
- Good team compliance through team meeting
- Privacy screens observed
- Control over sensitive PII database information
- Certification of training observed (17/05/2018)
- Password protection of attachments
- Key management

Effectiveness: The good objective evidence gathered in this section identified that planned objectives have been realised and planned results have been achieved

Physical & Environmental Security A.11:

Building is covered is mid terrace and has full CCTV coverage with applicable signage
Doors are controlled with proximity car readers issued to staff
Reception is staffed during building opening hours
Reception is located in a separate vestibule with secured doors leading to the main office locations
Internal doors and lifts are secured by proximity readers
Ground floor windows have shutter protection on the front of the building
Server room segregated and restricted access via pin lock
Confidential waste bins (all locked) in every office
Separate post room in place (See NCR to this section)

PAT Testing
- Swifts carried out testing on 09/02/2018 certificates 2913, 2915 and 2916

Alarm Systems
- Secom carried out servicing on 04/01/2018 certificate 2042582

Access Control
- Secom carried out servicing on 23/04/2018 certificate 4884412

CCTV
- Secom carried out servicing on 11/05/2018 certificate 4994127
- CCTV system is time synchronised
- 8 cameras in operation on month overwrite
- Access requests are made via the Information Governance manager

Emergency Fire testing
- Elite Fire carried out servicing on 29/03/2018 certificate 181565
- Fire alarm tests carried out weekly
- Full list of fire tests were evidenced going back to 2014
- Fire evacuation records for 19/09/2017 and 12/06/2017 were viewed; tests successful
- Chubb inspection for panels serviced 18/01/2018 certificate 27907778

- Chubb serviced fire extinguishers in 05/2018 and they are scheduled for service prior to end of month

Air Conditioning
- Ensys carried out servicing 24/04/2018 certificate 80662

Gas Safety
- Under Control Ltd carried out a gas safe inspection on 21/11/2017 certificate 298

Confidential Waste Removal
- Restore Datashred (PHS) are utilised for weekly collections
- Certificates for collections on 15/05/2018 and 08/05/2018 certificates 237152522 and 237140264
- Restore Datashred ISO27001 Certificate viewed - IS610091

Effectiveness: With the Minor Non conformance raised in this section, it is identified that planned objectives have not been fully realised and results have not been fully achieved.

Business Continuity A.17:

Planning
- Business Continuity Management DOC A17, v1.7 dated 17/05/2018 was viewed
- IS clearly articulated with objectives set
- Disaster Recovery for the restore of principle IT systems, REC 17A, v1.5 dated 27/03/2018 was viewed
- Business Continuity Plan is in place and stored on Shadow Planner (continual updates)
- Main plan breaks down into individual business functions
- Test of the use of Shadow Planner was last undertaken on 01/02/2017
- Test of the BCP is currently postponed until a the new business structure is formalised and embedded. Once embedded a forward testing will be produced.
- Business Continuity Risks were reviewed in the Risk Register at entries 3.3, 9.13, 2.1, 9.9, 2.4 and 9.15
- These risks have been considered in the BCP within Shadow Planner

Testing
Tests have been undertaken to test the IT recovery plan. Records were observed of tests:
- Test records for Continuim BD on 18/10/2018
- Test record for PMP02 (password manger) on 20/02/2018
- Test record for RSSQL on 07/02/2017

Actions from these tests follow the documented RAID process

Redundancy
This was observed in:
- Capacity reports
- Azure site recovery services in place and dashboard viewed and showed healthy state

Effectiveness: The good objective evidence gathered in this section identified that planned objectives have been realised. However, please note the additional opportunity for improvement.

Finding Reference	1630565-201805-I2	**Certificate Reference**	IS 600771
Certificate Standard	ISO/IEC 27001:2013	**Clause**	A17.1.3
Category	Opportunity for Improvement		
Area/process:	Business Continuity A.17		
Details	Notwithstanding the evidenced IT recovery tests the major corporate BCP in Shadow Planner was last exercised in early 2017. It has not been initiated since then. The new internal business realignment, once fully implemented, will then allow for a forward plan of tests to occur. The organisation should plan these tests at the earliest opportunity.		

Security Incident Management A.16:

Incident Management, DOC A16, v1.7 dated 18/05/2018 was viewed
- Document includes reporting, responsibilities for investigation and collection of evidence

Information Incident rating Process, DOC A16.2, v1.3 dated 27/03/2018 was viewed
- This document outlines how incidents are rated with respect to harm to the business or individual

Incidents Reported
- 58 incidents have been recorded since July 2017
- Incidents have been reported to the EMT to give annual breakdown
- Viewed document revealed a full incident analysis for 06-07/2017 presented

Incidents sampled
- IIR 10.218 dated 16/02/2018
- IIR 16.2018 dated 09/03/2018
- IIR 19.2018 dated 16/03/2018
- IIR 28.2018 dated 17/05/2018

All incidents have clearly followed process for consistency and have been fully evaluated with evidence collected to support the investigation reports.

Effectiveness: The good objective evidence gathered in this section identified that planned objectives have been realised and planned results have been achieved

Supplier Relationships A.15:

Suppliers & Agreements
- Supplier Relationships, DOC A15, v2.4 dated 17/05/2018 was viewed
- Document required that suppliers are to have information security policies and procedures appropriate to the nature of the HCPC data they handle
- A risk table is included against the levels, and types, of data held by the supplier giving a risk profile of High to Very Low
- A full list of data protection and information security clauses are included in the above document for inclusion in contracts for data held. This may not be used if the supplier included confidentiality clauses in their offering of service. These clauses are reviewed by the organization's legal counsel
- A full list of suppliers was viewed within a maintained database

- Procurement guide now requests new suppliers are ISO27001 certified
Suppliers sampled include:
- Law Absolute
- Xerox
- Core Computer Consultants (Core HR)
- Kingsley Napley

Contracts contains elements of Data Protection, Confidentiality and IPR, and additionally, as a Security Management Plan for Xerox

Monitoring
- Suppliers are vetting in line with Appendix 1 to the above document
- A review of all suppliers, by cost spend, took place in 01/2018 with a relationship manager assigned
- Procurement manual sets out how and when suppliers are to be reviewed against risk

Additional service review meetings

- Xerox have quarterly review meetings; record of 04/2018 meeting observed
- Monthly review meetings take place with Kingsley Napley; minutes of meeting 26/04/2018 were observed

Effectiveness: The good objective evidence gathered in this section identified that planned objectives have been realised. However, please note the additional opportunity for improvement.

Finding Reference	1630565-201805-I3	**Certificate Reference**	IS 600771
Certificate Standard	ISO/IEC 27001:2013	**Clause**	A15.2.1
Category	Opportunity for Improvement		
Area/process:	Supplier Relationships A.15		
Details	Although evidence of supplier review was evidenced the organization could enhance these by the addition of Information Security specific clause reviews as part of the process by the relationship manager		

Update of 3-year plan and agree dates for next visit:

The dates for the next visit cycle, in beginning in 2019, have been agreed with the client along with the additional days required as part of the ISO27006 durations calculator.

Minor (3) nonconformities arising from this assessment.

Finding Reference	1630565-201805-N1	**Certificate Reference**	IS 600771
Certificate Standard	ISO/IEC 27001:2013	**Clause**	7.5.2
Category	Minor		
Area/process:	ISMS policy and procedures, internal audits, corrective action. 5, 7, 9,10		
Statement of non-conformance:	Documents appearing in the live ISMS on the organization's intranet were viewed as being in draft format having not received formal approval from the Executive Leadership Team		
Clause requirements	Creating and updating When creating and updating documented information the organization shall ensure appropriate: c) review and approval for suitability and adequacy.		
Objective evidence	A number of documents within the ISMS on the intranet were noted to be in Draft format and had not been formally approved by the Executive Management Team. This is contrary to the organisations ISMS manual and was agreed with the guide.		
Cause			
Correction / containment			
Corrective action			

Finding Reference	1630565-201805-N2	**Certificate Reference**	IS 600771
Certificate Standard	ISO/IEC 27001:2013	**Clause**	10.1
Category	Minor		
Area/process:	ISMS policy and procedures, internal audits, corrective action. 5, 7, 9,10		
Statement of non-conformance:	Non conformities raised at internal and external audits have not effectively had the root cause determined to see if further nonconformities exist or the effectiveness of the corrective actions analysed.		
Clause requirements	Nonconformity and corrective action. When a nonconformity occurs, the organization shall: 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	Improvement Log Entries 417 and 516 are interlinked and are showing as being closed. Neither entry has a root cause assigned. A check to see if this nonconformity is occurring elsewhere and the review of effectiveness has not taken place.
Cause	
Correction / containment	
Corrective action	

Finding Reference	1630565-201805-N3	**Certificate Reference**	IS 600771
Certificate Standard	ISO/IEC 27001:2013	**Clause**	7.5.3
Category	Minor		
Area/process:	Physical & Environmental Security A.11		
Statement of non-conformance:	The control of incoming and outgoing mail was not effectively controlled.		
Clause requirements	Control of documented information Documented information required by the information security management system and by this International Standard shall be controlled to ensure: b) it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity).		
Objective evidence	It was observed that open outgoing mail bags, containing mail, were left in the main reception area. This did not offer adequate protection of theft of mail from either an insider or visitor to the building. It was further noted that incoming mail was stacked on the reception desk being scanned upon receipt. Whilst the mail was not opened at this point there was little protection offered against the potential of theft from an internal or external source. This was agreed with the facilities team guide. Sampled incident IIR19.2018 is evidence that mail can be lost in the reception area.		
Cause			
Correction / containment			
Corrective action			

Next visit objectives, scope and criteria

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

The scope of the assessment is the documented management system with relation to the requirements of ISO27001 and the defined assessment plan provided in terms of locations and areas of the system and organization to be assessed.

The criteria of the assessment are BS EN ISO27001:27001 in relation to Health and 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 organization 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.

Next visit plan

Date	Auditor	Time	Area/process	Clause
29/04/2019		0900	Opening Meeting	
		0930	Review previous report, confirm status of ISMS and scope	
		1000	Context of the Organisation, Scope and Policy	
		1045	Leadership and Commitment	
		1130	Objectives / Performance Monitoring & Measurement	
		1230	Lunch	
		1315	Planning and Resources	
		1400	Internal Audit, Corrective Actions, Management Review	
		1500	Supplier Relationships	
		1600	Interim Meeting	
30/04/2019		0900	Review of previous day	
		0915	Risk Assessment, Risk Treatment, Statement of Applicability	
		1030	Operations Security	
		1130	Physical and Environmental Security	
		1215	Lunch	
		1300	Security Incident Management	
		1345	Human Resource Security	
		1430	Registrations (Awareness Sampling)	
		1500	Policy & Standards (security awareness sampling)	
		1530	Education Team (security awareness sampling)	
		1600	Closing Meeting	
01/05/2019		0900	Off site follow up of audit trails	
		1000	Report Writing (0.5 day off site)	

Appendix: Your certification structure & on-going assessment programme

Scope of certification

IS 600771 (ISO/IEC 27001:2013)

The management of 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 SoA v1.7 dated 16/05/2018.

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	Re-certification Audit (RA Opt 2)
Assessment reference	8704384
Assessment dates	21/05/2018
Deviation from audit plan	No
Total number of Employees	250
Effective number of Employees	250
Scope of activities at the site	Change to version number and date
Assessment duration	4.5 day(s)

Certification assessment programme

Certificate number - IS 600771
Location reference - 0047125084-000

		Audit1	Audit2	Audit3	Audit4	Audit5
Business area/location	**Date (mm/yy):**	05/18	05/19	05/20	04/21	04/21
	Duration (days):	4.5	3	3	0.5	6
Continuing Assessment			X	X		
Triennial Recertification		X				X
Context of the Organisation, Scope and Policy		X	X	X		X
Leadership and Commitment		X	X	X		X
Planning and Resources		X	X			X
Human Resource Security		X	X	X		X
Control of Documents and Records		X		X		X
Objectives / Performance Monitoring & Measurement		X	X	X		X
Internal Audit, Corrective Actions, Management Review		X	X	X		X
Supplier Relationships		X	X			X
Risk Assessment, Risk Treatment, Statement of Applicability		X	X	X		X
Compliance: Legal and Other Requirements		X		X		X
Security Incident Management		X	X			X
Access Control & Cryptography		X		X		X
Physical and Environmental Security		X	X			X
Asset Management		X		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
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		X
Communications Team (security awareness sampling)	X		X		X
Project Management Team (security awareness sampling)	X		X		X
Programme Management		X	X	X	

Mandatory requirements – recertification

Review of assessment finding regarding conformity, effectiveness and relevance of the management system:

The organization was noted to be continuing to maintain and improve the processes effectively with particular regard to the following areas:
- Education and awareness of staff
- IS consideration in project management

However, there are further possible Opportunities for Improvement which will reduce risk and assist with achieving the intended result:
- Closure and evaluation of NCRs
- Publishing of draft documents

Management system strategy and objectives:

It is expected that the ISMS will mature further over the next cycle and will continue to improve with commitment from those involved

Review of progress in relation to the organization's objectives:

Top management have demonstrated key strategic direction of the organization and fully understood the IS risks which are being carried.

The restructuring of the organization's Senior Leadership was discussed. This allows the flexibility for the business to grow in line with its strategic direction.

Key risks included:
- Cyber attack
- Loss of registrant details

It was clear that there are regular meetings, and reporting mechanisms, in place to keep the Senior Leadership up to date with security strategy and the ability to clearly drive, from Senior Leadership down, a business culture which reflects the the organizations IS requirements and those of its registrants.

Review of assessment progress and the recertification plan:

During this recertification full coverage of all clauses were covered and these will be split over the next CAVS prior to full coverage again in the next recertification visit.

ISO27006 calculation was run with the BPI Manager and Chief Executive and they have both agreed that due to the nature of the business, and the roles conducted by staff, then all are integral and must be included in the calculation. This has been reflected in an increase of days for the next cycle.

BSI client management impartiality and surveillance strategy:

The relevant P and T codes associated with this client still remain and are pertinent. Impartiality has been maintained and a new auditor will be assigned to the next cycle due to this auditor covering the Scotland territory. Currently the organization are working from one building but works are in place to expand into the next building. It is anticipated both buildings will be interconnected and will operate as one.

Continue with the current total assessment days/cycle.

Definitions of findings:

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.

How to contact BSI

'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

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 organization, then all pages must be included.

BSI, its staff and agents shall keep confidential all information relating to your organization 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.