Audit Committee, 17 June 2015

BSI ISO 27001:2013 Assessment Reports

## Executive summary and recommendations

### Introduction

BSI assessed HCPC on the 31 March and again on 20-22 May 2015, as part of the ISO27001:2013 initial certification process.

The two assessment reports are attached. One non-conformance was recorded in March, and two in May. A few Observations were recorded. These are detailed in the reports attached.

HCPC have been recommended for certification to ISO27001:2013. This should be confirmed within 6-8 weeks of the Stage 2 audit.

### Decision

Committee is asked to note the report.

### Background information

None

### Resource implications

None

### Financial implications

None

### Appendices

BSI 2015 STAGE 1 ASSESSMENT REPORT, ISO27001:2013.
BSI 2015 STAGE 2 ASSESSMENT REPORT, ISO27001:2013.

### Date of paper

5 June 2015

# Assessment Report.

## Health & Care Professions Council

| | |
|---|---|
| **Report Author** | **Kwadwo Anim-Appiah** |
| Visit Start Date | 31/03/2015 |



...making excellence a habit.™

# Introduction.

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

| Visit ref/Type/Date/Duration | Certificate/Standard | Site address |
|---|---|---|
| 8258092<br>Stage 1 Audit<br>31/03/2015<br>2 day(s)<br>No. Employees: 215 | IS 600771<br>ISO/IEC 27001:2013 | Health & Care Professions Council<br>Park House<br>184 Kennington Park Road<br>London<br>SE11 4BU<br>United Kingdom |

The objective of the assessment was to determine the organisation's readiness for the stage 2 audit and to ensure its effective planning.

# Management Summary.

**Overall Conclusion**

**I am pleased to confirm your readiness to go for Stage Two assessment**

The nonconformity identified will need to be addressed before the next stage of assessment and will be reviewed in Stage Two

**The stage 2 assessment duration is planned to be 4.5 days but will be conducted in a 3 days with 2 Assessors. As a result of this visit the duration is to be reviewed and confirmed by our Sales department.**

The objectives of this assessment have been achieved.

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

Based on the objective evidence detailed within this report, the areas assessed during the course of the visit were generally found to be effective.

There were no outstanding nonconformities to review from previous assessments.

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

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

**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 08/04/2015 by e-mail to msuk.caps@bsigroup.com or by fax to +44 (0)1908 228123, referencing the report number.**

# Mandatory Requirements.

# Areas Assessed & 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.

**Company Overview – Organisation Context, Interested Parties and Scope / Leadership / Compliance : 4.1, 4.2, 4.3, 5.1, A.18**

Health & Care Professions Council (HCPC) regulate the following professions: arts therapists, biomedical scientists, chiropodists / podiatrists, clinical scientists, dieticians, hearing aid dispensers, occupational therapists, operating department practitioners, orthoptists, paramedics, physiotherapists, practitioner psychologists, prosthetists / orthotists, radiographers, social workers in England and speech and language therapists. The professional titles used by these professions are protected by law.

HCPC regulates about 320,0000 registrants. HCPC is neither public nor a private sector organisation. HCPC is independent of Government. HCPC regulates over 16 medical professions. 800 different approved programmes available to registrants. Registrants are also required to meet statutory requirements. HCPC has a turnover of about £25M. HCPC stores both paper-based and electronic-based data.

Interested parties have been identified which include registrants, partners, regulated educational establishments, consultants etc. Their needs and expectations have been clearly captured within HCPC's ISMS Manual. The Chief Executive and Registrar has the overall authority and responsibility for the ISMS.

Documents reviewed included:
1. DOC 18 Compliance & Redundancies v1 (23/01/2015)
2. DOC A1 ISMS Manual
3. REC15 1 List of Legislation & Regulation v2
4. Risk Register & Risk Treatment Plan (Feb 2015)

**Management System, Policies and Objectives, Documented Information Organisational Planning and Control : 4.4, 5.2, 5.3, 6.2, 7.5, 8.1**

The Information Security Policy reviewed covers all the requirements of clause 5.2. Overall responsibility lies with the Chief Executive & Registrar. Authority has been delegated to the Executive Management Team (EMT). All ISMS relatd documents sampled was well versioned with references. HCPC has an established Information Security Group that reviews the ISMS. The Head of Business Improvement also acts as the Information Security Manager. HCPC holds the 9001 certification and as such has a matured processes. ISMS related documents are held on HCPC's intranet.

HCPC has a supplier management policy that governs outsource processes and procedures. HCPC's Acceptable Use Policy (AUP) can be found within the IT Policy form. All employees are required to sign the IT Policy Form.

Information Security Objectives were reviewed. Clear metrics have been set showing timelines for those that are practicable. However, it was unclear who the owners of these objectives were. A non-conformity has been raised in relation to this. Please see the relevant section for further details.

Roles and responsibilities have been clearly defined. Information is classified into 4 levels and these are:

- Unrestricted
- Restricted
- Confidential
- Highly Confidential

Documents reviewed included:
1. DOC A5 Information Security Policy (22/02/2015)
2. DOC A3 Effectiveness Measures
3. DOC A6.1 Organisation of the ISMS (19/02/2015)
4. DOC A15 Supplier Relationships (23/01/2015)
5. DOC A8.2 Information Classification & Handling Policy
6. IT Policy Form

**Tour Facility : A.11**

HCPC occupies 3 buildings at the same site. Visitors are issued a visitors' badge. Once the visitor gets to the premises, they are issued a visitors' badge and collected by an employee in order to gain access to the office area. It was observed that printers require the touch of an employee's issued card to release jobs. The office environment was very neat and tidy. Clear desk and clear screen was seen to be adhered to. No tail gating was observed. Confidential waste bins are well placed at vantage points within the building. Fire exits were free of any obstruction and fire extinguishers were found to have been tested. Card access is required for all entrances. Fire extinguishers inspected have been tested and still in date. Cabinets holding records are lockable.

The server room was inspected. It was tidy and the cables to the switches have been well tied up. An observation was raised with regards to the presence of cardboard boxes within the server room. The server room has fire alarms and well air conditioned. HCPC also have in place a flood protection barrier in the basement to prevent ingress.

# Observations.

| Type | Area/Process | Clause |
|---|---|---|
| Observations | Tour Facility | |
| Scope | IS 600771 | |
| Details: | Some combustible materials in the form of cardboards were seen in the server room. | |

# Opportunity for improvement.

| Type | Area/Process | Clause |
|---|---|---|
| Opportunity for improvement | Tour Facility | |
| Scope | IS 600771 | |
| Details: | HCPC may wish to consider removing individual bins near desks and rather make use of the designated segregated bins to avoid the possibility of an employee discarding confidential waste into the side bins by desks. | |

**Senior Management (if possible) : 5, A.5**

The Director of Operations was interviewed to gauge top management's commitment to the ISMS and also HCPC's drivers for certification. Drivers include: Assurance to registrants and the general public; securing personal/sensitive data; protection and preservation of CIA; implementing appropriate controls etc According to the Director of Operations, HCPC considers the following as the biggest risks to the ISMS:

- Not securing personal data of registrants
- Unable to embed information security awareness into HCPC's culture
- Human error

As a business, Management has ensured that its information policy and objectives reflect its strategic direction. The needs of the business informed the setting of the objectives. The objectives, policies etc are all channelled to employees through the Executive Management Team (EMT). Please note that the Director of Operations explained the overview of the company and its context. The import of this can be read in the above section on "Company Overview".

**Risk Assessment – General Information Security Risk Assessment / Information Security Risk Treatment and Statement of Applicability : 6.1.1, 6.1.2, 8.2, 6.1.3, 8.3**

The organisation maintains a risk assessment & treatment document. The risk assessment & treatment document was reviewed. Risks have been identified, analysed, evaluated and treated using a criteria. The risk methodology used is well structured. Owners have been assigned to identified risks with clear criteria and guidelines. HCPC uses 3rd party tool "VSRisk" in managing its initial risks, treatment and SOA. HCPC also manages its risk in a manual document.

The SOA reviewed dated 22/01/2015 included control objectives and the controls selected with reasons for their selection as mandated by the standard. Inclusions and their justifications have been clearly stated. Selection of controls are based on contractual requirements, legal/regulatory requirements, best practice, business reasons etc.

HCPC has no exclusions.

Some of the risks sampled included:
- Loss of reputation (medium)
- Interruption to electricity supply (high)
- Basement flooding (medium)

Appropriate treatment and mitigation has been applied to the above identified risks.

Documents reviewed included:
1. Risk Register & Risk Treatment Plan (Feb 2015)
2. DOC A2 Risk Management v1.1 3/2015)
3. Risk Assurance Mapping
4. Statement of Applicability for ISO 27001:2013 v1 (22/01/2015)
5. Audit Committee Meeting Management Strategy & Processes (19/03/2015)
6. Internal Audit Report Lead (23/03/2015)
6. Risk Management Process

# Observations.

| Type | Area/Process | Clause |
|---|---|---|
| Observations | Risk Assessment – General Information Security Risk Assessment / Information Security Risk Treatment and Statement of Applicability | 6.1.3 |
| Scope | IS 600771 | |
| Details: | There was no evidence that residual high level risks have been signed off. However, this could not be raised as a non-conformance because on 23/03/2015, ITG conducted an internal audit on behalf of HCPC and this was picked up as per clause 6.1.3f. HCPC is yet to review this in the next review meeting. HCPC must ensure that mechanisms are in place to ensure that high residual risks or high risks in general are signed off appropriately. | |

**Context of the Organisation : Clause 4**

The Context of the organization has been defined within the ISMS manual and articulates the internal interfaces which include (Education: Communications: Finance: Fitness to practice:: HR IT: Operations: Policy & Standards: Post Delivery: Secretarial & Customer Service and Council): Council, and the Third party interfaces include ( Suppliers: Partners: Software Licensing: Consultants Professional Services: Landlord: Local Authority: Hosting Suppliers: Telecomms: Professional Service Suppliers and Regulator). The needs of the these interested parties has been considered and the system scope is seen to to be appropriate to the business needs and any issues identified have been directly feed into the risk assessment.

**Resources : 7.4**

Defined resources and consultancy services have been available for the implementation of the ISMS project. Resource are also in place for the ongoing support of the ISMS and responsibilities have been allocated for the management of Information Security. All staff have job descriptions and the minimum skill level for each position has been defined allowing staff competencies to be determined and reviewed

Staff screening relies mainly on two completed references, however some of this can be limited and there may be benefit from looking at a more effective way of conducting staff background checks E.G. DBS .

All staff complete CBT training on Information security and there is a security culture developing with the use of posters and security campaigns.
- Lots of security posters distributed through the company.
- Action Forms List: to be used when employees do not comply with security rules; different templates, depending on the issue.

**ISMS monitoring : 9**

IT systems are monitored and a monthly report identifying pertinent measures for IT systems, the overall view of IT is a well controlled and mature operation.

Management Review
A comprehensive monthly meeting is completed and this forms the bases of the management review as all the requirements from the standard are included in the monthly meetings.

Internal audits
A programme of internal audits have been established and date back longer than the minimum three month period.

**Incident Management :**

A documented procedure A16 defines the process to be followed when reporting security incidents, the initial impact and response required is considered and then the incident is passed on to the security team who will investigate and compile a report. all incidents are then summarised in a monthly security incident report provided to the EMT Executive Management Team. A16 23/3/15

**BCP :**

A business Impact analysis has been completed to identify the critical services, from this a BCP plan has been developed which provides the response to several scenarios. A war box is available which holds key information and contacts to allow a crises to be initially managed. The lans supporting the top level BCP plan were not viewed and no review of any testing has been undertaken and will need to be verified at the stage two assessment. A17 2/2/15 verified

**Supplier Relationship :**

Engagements with third party requires a confidentiality agreement to be signed before any services can be supplied. All contracts contain security requirements and new suppliers undergo an audit before approval. Performance is monitored and no third party supplier has direct access to the information of HCPC. Procedure A15 23/1/15 verified..

**Closing Meeting :**

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

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

# Minor Nonconformities Arising from this Assessment.

| Ref | Area/Process | Clause |
|---|---|---|
| 1174100N1 | Management System, Policies and Objectives, Documented Information Organisational Planning and Control | 6.2 |
| Scope | IS 600771 | |
| Details: | Information security requirements not fully met | |
| Requirements: | Information security objectives and planning to achieve them<br>The organization shall establish information security objectives at relevant functions and levels.<br>The information security objectives shall:<br>a) be consistent with the information security policy;<br>b) be measurable (if practicable);<br>c) take into account applicable information security requirements, and results from risk assessment and risk treatment;<br>d) be communicated; and<br>e) be updated as appropriate.<br>The organization shall retain documented information on the information security objectives.<br>When planning how to achieve its information security objectives, the organization shall determine:<br>f) what will be done;<br>g) what resources will be required;<br>h) who will be responsible;<br>i) when it will be completed; and<br>j) how the results will be evaluated. | |
| Objective Evidence: | The Information Security Objectives reviewed was silent on who will be responsible for achieving the objectives set. The objectives reviewed had some metrics (for those that were measureable), but it was difficult to ascertain whose responsibility it was to achieve the objectives as listed. HCPC must ensure that the requirements of clause 6.2 are fully met, especially 6.2i. | |

# Assessment Participants.

On behalf of the organisation:

| Name | Position |
|---|---|
| Roy Dunn | Head of Business Process Improvement |
| Greg Ross-Samson | Director of Operations |
| Ian Shorten | Information Risk Consultant |
| Kayleigh Birtwistle | Quality Compliance Auditor |
| Kim Wilcox | HR Advisor |
| Rici Wellsby | IT Service Support Manager |

The assessment was conducted on behalf of BSI by:

| Name | Position |
|---|---|
| Kwadwo Anim-Appiah | Team Leader |
| Irvine Taylor | Team Member |

# Next Visit Plan.

**Visit objectives:**

Stage 2
The objective of the assessment is to conduct a certification assessment 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 and to confirm the forward strategic plan.

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

A plan for the Stage 2 visit will be provided to the organisation following the programme management planning day on 15/04/2015.

**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.**

# Notes.

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

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

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

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

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

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

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

Tel: +44 (0)845 080 9000 Fax +44 (0)1908 228123

Email: MK.Customerservices@bsigroup.com

# Assessment Report.

## Health & Care Professions Council

**Report Author** **Kwadwo Anim-Appiah**

Visit Start Date 20/05/2015



...making excellence a habit.™

# Introduction.

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

| Visit ref/Type/Date/Duration | Certificate/Standard | Site address |
|---|---|---|
| 8258093<br>Stage 2 Audit<br>20/05/2015<br>4.5 day(s)<br>No. Employees: 240 | IS 600771<br>ISO/IEC 27001:2013 | Health & Care Professions Council<br>Park House<br>184 Kennington Park Road<br>London<br>SE11 4BU<br>United Kingdom |

The objective of the assessment was to conduct a certification assessment 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 and to confirm the forward strategic plan.

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

**Proposed scope of registration IS 600771 (ISO/IEC 27001:2013)**

| Location | Scope |
|---|---|
| Health & Care Professions Council<br>Park House<br>184 Kennington Park Road<br>London<br>SE11 4BU<br>United Kingdom | 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 to the Statement of Applicability version 1.2 dated May 2015. |

# Management Summary.

**Overall Conclusion**

**Congratulations! We are pleased to recommend that the scope of activities detailed in this report meet certification requirements.**

The recommendation is made subject to submission and acceptance of the client's corrective action plan.

The recommendation will be independently verified within BSI. Upon verification your certificate of certification will be issued.

The objectives of this assessment have been achieved.

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

Based on the objective evidence detailed within this report, the areas assessed during the course of the visit were found to be effective.

HCPC must be commended for adopting the "Privacy Impact Assessment" as prescribed by the ICO and this will be embedded in all projects going forward. Being in a regulated industry, HCPC has shown commitment to the ISMS and ensured that their processes and procedures also meet the requirements of the ICO. HCPC has a maturing system partly due to the fact that it holds ISO 9001 certification. It was visible that a lot of work had gone into information security awareness as this was demonstrated during the sampling of the staff in all the departments. The information security team must be commended for the hard work done.

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

2 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 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 01/06/2015 by e-mail to msuk.caps@bsigroup.com or by fax to +44 (0)1908 228123, referencing the report number.**

# Mandatory Requirements.

# Areas Assessed & 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.

**Context of the organisation: internal/external issues and interested parties / Legislation and compliance / Objectives and targets : 4, 5, 6, A.18**

Health & Care Professions Council (HCPC) regulate the following professions: arts therapists, biomedical scientists, chiropodists / podiatrists, clinical scientists, dieticians, hearing aid dispensers, occupational therapists, operating department practitioners, orthoptists, paramedics, physiotherapists, practitioner psychologists, prosthetists / orthotists, radiographers, social workers in England and speech and language therapists. The professional titles used by these professions are protected by law.

HCPC regulates about 320,0000 registrants. HCPC is neither public nor a private sector organisation. HCPC is independent of Government. HCPC regulates over 16 medical professions. 800 different approved programmes available to registrants. Registrants are also required to meet statutory requirements. HCPC has a turnover of about £25M. HCPC stores both paper-based and electronic-based data.

Interested parties have been identified which include registrants, partners, regulated educational establishments, consultants etc. Their needs and expectations have been clearly captured within HCPC's ISMS Manual. The Chief Executive and Registrar has the overall authority and responsibility for the ISMS.

HCPC has identified its interested parties and their requirements. These have been captured within HCPC's ISMS Manual. The manual also contains HCPC's scope which fully meet the requirements of the standard. Activities and boundaries and their inter-relationships have been determined. Internal and external issues can be found within HCPC's risk register. Objectives reviewed now fully meet the requirements of the standard. A non-conformity on this was raised during stage 1 assessment.

Legal and regulatory requirements have been duly captured. IT and information security related policies and procedures were seen to be in place. Information classification and handling policy remains the same as reviewed during the last assessment. HCPC has put in place measures to move away from Lotus Notes email client and rather deploy Microsoft Outlook. This will enable HCPC ensure that default classification and retention of emails are implemented.

Roles and responsibilities have been clearly defined and it was noted that the CEO/Registrar has the overall responsibility for the ISMS. All ISMS related documentation are stored on HCPC's intranet with the exception of A.12 Control documentation. Confidential information are stored on restricted shared drive.

Documents reviewed included:
1. DOC A5 Information Security Policy v1.1 (28/04/2015)
2. DOC A3 Effectiveness Measures (02/04/2015)
3. DOC A1 ISMS Manual v1.3 (28/04/2015)
4. DOC A8.2 Information Classification & Handling Policy
5. DOC A8 Compliance & Redundancies v1.1 (28/04/2015)
6. REC18 1 List of Legislation and Regulation v2
7. REC 6.1A Roles & Responsibilities

8. DOC A6.1 Organisation of ISMS (28/04/2015)
9. DOC A11.2.9 Tidy Desk Policy
10. DOC A7 HR Security

**Review previous report, confirm status of ISMS and scope :**

The outstanding non-conformity on Information Security Objectives was seen to have been rectified and this was closed accordingly. HCPC's scope statement was confirmed and updated with the latest version of its SOA. No major changes were recorded.

**Risk management, and statement of applicability / Asset management : 6, 8, A.8**

HCPC maintains a single inventory of information assets which is subdivided by asset owners into separate asset groups. Changes to identified risks are reviewed and agreed at the monthly Executive Management Team meetings (this also serves as the Management Review Meetings). Residual risks are implicitly accepted for current risks at EMT meetings.

The organisation maintains a risk assessment & treatment document. This well reviewed during stage 1 assessment and also in this assessment. The focus now was to look at HCPC's implementation of its risk assessment and treatment process. Risks have been identified, analysed, evaluated and treated using a criteria. The risk methodology used is well structured. Owners have been assigned to identified risks with clear criteria and guidelines. HCPC uses 3rd party tool "VSRisk" in managing its initial risks, treatment and SOA. HCPC also manages its risk in a manual document and the outcome forms part of the monthly report for the EMT.

The SOA reviewed dated 11/05/2015 included control objectives and the controls selected with reasons for their selection as mandated by the standard. Inclusions and their justifications have been clearly stated. Selection of controls are based on contractual requirements, legal/regulatory requirements, best practice, results of risk assessments etc. Related documents have been referenced within the SOA.

HCPC has no exclusions.

Top risks are highlighted and discussed at EMT meetings.

Some of the risks sampled included:
- Loss of reputation (medium)
- Interruption to electricity supply (high)
- Basement flooding (medium)
- PSA full cost recovery and significant financial impact (medium)
- Rapid increase in number of allegations (medium)

Appropriate treatment and mitigation has been applied to the above identified risks.

Documents reviewed included:
1. Risk Register & Risk Treatment Plan (Feb 2015)
2. DOC A2 Risk Management v1.2 (28/04/2015)
3. DOC A8.1 Asset Management
4. Statement of Applicability for ISO 27001:2013 v1.2 (11/05/2015)
5. Risk Management Process (28/04/2015)

**ISMS policy and procedures, internal audits, corrective action / Management review and monitoring of effectiveness of ISMS / Incident management : 5, 9, 10, A.16**

HCPC's internal audit programme (schedule) was reviewed. It was noted that audits are carried out on a monthly basis in order to meet requirements for ISO 9001 and ISO 27001. It was further noted that the audit programme did not just cover ISO 27001 requirements but also HCPC's own processes and procedures. According to HCPC, audits will be risk based after certification and previous reports will also inform the frequency of the audits.

Audit results are reviewed by the Executive Management Team (EMT) at HCPC's monthly management review meetings. Agenda items were seen to meet the requirements of the standard. Parts of the agenda also forms part of the Audit Committee meetings which is held 4 times in a year. This include risk management results, information security incidents and near misses/non-conformities. The last EMT meeting was held on 28/04/2015 and the next meeting is scheduled for 26/05/2015. The agenda for this meeting was reviewed.

HCPC maintains an improvement log. The log contains the following: incidents, non-conformities, near misses, and observations. The log also captures root causes and serves as HCPC's corrective action log.. However, it was noted that the log failed to capture the observations and non-conformity from the Stage 1 assessment. These could not be traced from the log.

Sampled incidents were:
- IIR43 Human error (incorrect address entered on NetReg) logged 08/05/2015
- IIR41 Un-redacted PII found in emails sent to CPD assessors (logged 29/04/2015)
- IIR36 Letter meant for registrant about non-payment of fees wrongly sent to registrant's employer (logged 28/04/2015)

Documents reviewed included:
1. Monthly Information Security Report
2. Incident Report - IT Department Door Maglock Compromise (23/03/2015)
3. Internal Audit Report - Tidy Desk 14/05/2015
4. Evaluation Report - Quality Assurance (Redaction Quality)
5. Near Miss Investigation Audit Report v1 (16/04/2015)
6. Audit Schedule v1.4 (14/05/2015)
7. Audit Committee Meeting Minutes (14/11/2014)
8. EMT Meeting Minutes & Agenda (28/04/2015)
9. REC MS_4A Improvement Log
10. DOC A16 Incident Management
11. Information Incident Report (19/03/2015)
12. Data Security - Incident Report Form
13. Council Meeting Minutes (14/05/2015)

**Business continuity / System acquisition, development and maintenance / Supplier relationships : A.17, A.14, A.15**

HCPC's Business Continuity Plan was reviewed and found to be well maintained. HCPC maintains a war box containing the BCP at the DR Site. HCPC has 10 seats available at a DR Site in Uxbridge. Access lists to the DR site was reviewed. The BCP is available to selected employees and council members in hard copy format. Tests are carried out on an annual basis. Results of tests were available for review. It was noted that last year's test was based solely on IT Systems. The scenario for the test was based on burst water main rupture, flooding BT pipe work carrying telecommunication lines. Key resources have been identified and similarly, RTO's and RTO's have been determined.

Development is outsourced. HCPC has controls in place and a policy for secure development which is adhered to by 3rd parties. Developers have restricted access to applications and support is provided via VPN. HCPC has escrow accounts and this is managed by

a 3rd party (NCC Group). System changes go through rigorous reviews by HCPC's CAB. Segregated test environments exists. Test data are protected and redacted.

HCPC has a policy for managing Supply Relationships. "Right to audit " clauses were noted in the agreements reviewed. HCPC has supplier monitoring as part of its audit programme. New projects are assessed against ICO's Privacy Impact Assessment. Suppliers are risk assessed based on the following:

- Information suppliers handle
- Volume of information
- Frequency of handling the information

The above determines the suppliers level of risk which is categorised as High, Medium or Low.

Documents reviewed included:
1. DOC A17 Business Continuity Management v1.2 (28/04/2015)
2. Brief Report For November 2012 Exercise
3. Annual Business Continuity Test - Audit Committee (March 2013)
4. Report for November 2013 Exercise
5. REC 17A Disaster Recovery/Business Continuity Order of Restoration of Principle IT Systems for HCPC
6. Access Lists for DR Sites
7. DOC A14 Systems Acquisition, Development & Maintenance
8. 3.0 Change Management & 3.1 Emergency Change
9. DOC A15 Supplier Relationship v2.0 (19/05/2015)
10. Consult CRM Master Services Agreement (19/12/2012)
11. Request for Proposal - Education Systems & Process Review
12. Single Licensee Software Escrow Agreement (with 3rd party NCC)
13. HCPC - Charter UK Agreement (07/05/2010)
14. Escrow Agreement for NetReg (August 2003)
15. HCPC - DSL DPA (22/04/2010)
16. Rackspace Contract Agreement

**Security Awareness Sampling - Secretariat, Finance, Project Management, Communications, Education Teams :**

The staff were sampled to ascertain their knowledge on information security and it was evident that all of them have been through the awareness training. All staff interviewed were able to demonstrate their knowledge on information security and how it relates to their role. The staff were aware of the need to have segregation of duties and had a firm understanding of classification of information requirements in place. They were able to point out where the relevant policies and other documentation related to the ISMS stored on their portal. They knew the reporting procedures for information security incidents. Overall their knowledge on information Security was satisfactory. Awareness records were sampled during the HR session earlier on in the assessment. Please see the relevant section on HR.

HCPC's Secretariat is responsible for Information Governance matters such as Data Protection, Freedom of Information and Subject Access Matter requests including training. As such it was noted that the team have a bias when it comes to Information Security Awareness. They were able to demonstrate their strong knowledge on the subject.

The Finance team have robust systems and controls to ensure the protection and preservation of confidentiality, integrity and availability of data they work with. Checks and balances on transactions were seen to be in place. Credit card details are not held beyond a day. The data is securely locked and processed the day after. After this all completed transactions are securely shredded and only unique identifiers and key information without full credit card details are held for archival and regulatory purposes. The team

have all completed their information security awareness training and this was ably demonstrated when a new starter was interviewed.

The other teams: Education, Project Management and Communications showed great awareness in data protection, confidentiality, clear desk and screen policy (Tidy Policy), information security policy and incident reporting. It was noted that the project management team have embedded information security as a requirement and will be adopting the privacy impact assessment as part of the RFP process going forward. The Communications team scrutinises all content from the various department to ensure that any information put out is free of confidential data. This process requires an approval by the council and legal. The team is also the point of contact if there are suspicions that unauthorised persons (such as Journalists) are "fishing" for information on hearings. Education department deals with the approval of degree programmes and mainly deal with higher institutions. Confidential details held include University staff CVs and these are restricted to limited staff within the department.

**Top Management Interview : 5, A.5**

Top Management interview took place with the Director of Operations and the Chief Executive/Registrar. The CEO made it clear that HCPC understands that it will take time for the ISMS to mature and be fully embedded into HCPC's own processes and procedures. The organisation is committed to continual improvement and this is bolstered by the fact that HCPC also holds ISO 9001 certification with BSI. Financial and Human resources have been committed to the ISMS. £20000 has been allocated to the management of the ISMS and 12 people have recently undergone BSI's Internal Audit Course.

The company maintains a monopoly privilege. Processes are in line with applicable legislation and 99% of the organisations processes are in the public domain so ISO certifications became the "obvious thing to do" in order to achieve continuous improvement and maintain "public trust". Standards were embedded to the company's procedures. The concept of being "Open and Transparent" is the company's motto. During the first year of implementation a constant push to people is expected to take place to comply with the policies and procedures and then within 4 yrs of implementation the aim is to become an automatic process and completely embedded in the normal way of business and become a culture of people "saying this is how we do it".

The main drivers for the certification were the legal, commercial and public requirements for data confidentiality, integrity and availability.

The organisation handles confidential information and the consequence to the customers in terms of breach or loss of information would be tremendous and the reputational aspects of such event could destroy the company.

Monthly reporting systems are in place to support the ISMS.
IS roles and responsibilities have been defined and monitoring bodies are in place.

The client is subject to the following internal / external audits:
PSA
NAO
Commercial auditors
Internal audits
Accreditation bodies

Accreditation facilitate the review process of the regulators and 3rd party independent assessments.

Resources:
Investment in money and time has been made from management and staff in terms of documentation and implementation of the standard and a budget is maintained for on going training and assessments.

High Risks identified during the meeting:
Data loss and the consequences of the loss
Lost of trust in people
Data breach / loss of control over the organisation
Misuse - mishandling of information

**Access Control / Communication Security : A.9 / A.13**

The Access control policy DOCA9.1 / V.1.1 / 28.04.2015 was seen to be in place
Access control process DOCA.9.2 / V.1.1 / 05.05.2015
Related documentation:
IS Policy
Starters and Leavers Process
Health and social work professions order 2001
IT Policy Access to the company's systems can be made only by authorised users

The access rights to applications take into account:
the classification levels of information
data protection and privacy legislation and any potential client contractual commitments
the need to know principle
everything is forbidden unless expressly permitted
any privileges that users actually need to perform their roles
user access requests are subject to formal authorisation and periodic review

Authentication mechanisms for the guest wireless network are applied for users and equipment
Control of user access to information services is enforced
The network with scope of this policy is that installed at the HCPCs premises
A Network Overview Diagram was seen to be in place. Servers are on their own virtual network, separated. Security authentication protocols are used for authorising access to networks.

User Access Management:
The Recruitment and employee change database was seen to include the new starters listed. The following sample was selected from the list was followed the process through for effectiveness:
Creating an account:
23/03/2015 Temporary agency worker
Line managers recruitment authorisation form with details regarding facilities (access control cards, hours of working, mobile, keys,), IT department (VPN, PC--laptop, Lotus notes, access levels. etc) as of 20/03/2015
Approved by HR as of 20/03/2015
Account create by IT as of 23/03/2015

Changing privileges:
Contract variation (used for roles change)
Registration Manager / 05.01.2015 / Internal move from Case Team Manager FTP to Registration Dpt
Form approved by the Line manager in 01.12
Approved by HR ion 02.12.2015
Approved by Finance 04.12.2015
Approve by the CEO 09.12.2015
#108855/14.01.2015/Mitel software implementation, phone extension, passwords and usernames.
Removal of privileges of previous account.

Users can be added to group following the system owner or data owner request (sample seen #109537/26.03.2015 #109438/18.03.2015))

Closing and account:
Leavers form 02.01.2015 / Facilities Supervisor
Requirements for leaving form included the following details:
Date started
Leaving date
Entry access card
Office key
Mobile phone / blackberry
IT equipment
Details regarding IT accounts
Signed off by line manager as of 10/12/2015
HR approved on10/12/2015
Account was disabled on 06/01/2015

Review of access rights take place via the recruitment and employee change data base and through the services desk via the ticketing system.
Review comments were seen in the event of termination of an account in the recruitment and employee change data base. The client may consider it beneficial to "Account has been disabled the leavers process will now be started" but not for the change roles

Password Management Process in the induction Usernames, Passwords and security
Password must contain upper and lower case letters and numbers of high level characters. passwords change on a monthly basis.

DOC A.6.2 Mobile systems / v.1.1 / 28.04.2015 (Smart phones, Laptops control, Tablet computers controls)
Remotely HCPC device and a corporate laptop are required for remote access. VPN client manager and Cisco is used for dual authentication.
Mobiles contain Token Code Cryptocard creates an 8 digit code that needs to be inputted into the VPN.

Laptops are hard-disk encrypted and hide the c-drive from the local machines. Information can not be saved in the c-drive and due to encryption physical access risks are minimised.
Blackberries can be wiped off remotely.

Data can only be transferred and saved on external media either through a white listed USB device and those devices are controlled by BPI and signed out. Downloading of data or applications for the web are blocked.

**Encryption : A.10**

Cryptography Policy A.10 / V.1.2 /28.04.2015
the IT director is responsible for authorising any changes. HCPC encrypts data as required on a risk based approach. 128 bit encryption is the current standard for all encryption in the company. A secure password store is used to store encryption keys for all encrypted datasets or objects. Key generation is managed by the IT department using suitable tools and methods. For the public facing websites, key generation is carried out by an independent certificate authority. The policy for transfer of files via removable media and email is covered in he IT Policy.

Where encrypted files are sent to outside organisations, password should be communicated in a secure manner.

KeyPass application is used for Key management for the systems.

**Operations Security : A.12**

Operations security / DOC A.12 / v.1.2 / Highly Confidential / 28.04.2015
Change management.
The process was illustrated in the change management diagram work flow. Change management is initiated by a Change Request Form monitored by the CAB meetings on weekly basis. CAB agenda of the CAB s is maintained and reviewed . CAB takes place for reviews and approvals, port reviews and process reviews.
Sample seen RFC no #20150055/05.05.2015 details, priority, system owner, system to be changed, reasons for change, description for change, analysis of job to be performed, implementation plan, test plan with expected results, back out plan, testing, impact, guides, network diagram, impact on BCP or systems and reporting, licence requirements, security implications, risk analysis on the impact to the business and the likelihood, scoring, approval-comments, CAP review, Post Change Review / lessons, Post changing documents.

Development is outsourced to a 3rd party provider.

Symantec antivirus is used locally and uses messagelabs to scan incoming and outgoing emails. There is a current move of the organisation to Office 365.

DOC17 Provides evidence for the BC in regards Backups. Back ups are taken every 15 minutes to servers, daily backups, month end back ups. Tapes are kept offsite to a 3rd party.

The following System audit reports were reviewed:
Availability report
Failure back up report
Symantec cloud report anispam, antivirus, data protection
Symantec endpoint protection manager report

Service desk provides logging and monitoring services through the ticketing system. (sample seen #109537/26.03.2015 #109438/18.03.2015, # 110109/13.05.2015).

**Physical Security : A.11**

The client occupies 3 buildings around the Kennington area. The following controls were seen to be in place:
Manned entrance
Visitors Log
Coloured lanyard cards
Secure print
Shredders
Secure waste bins
Double entrance doors
CCTV surveillance system
Access control buttons on doors
FOB access to Stannery Street building
Filing cabinets
Fire alarm system
Intruders alarm system
Computer locks
Swipe on / off cards to doors and elevators
Safe storage boxes to transfer information
Security bars on windows

Fire extinguishers
Screen blockers in the Registration area
Limited access to computer room.

The following maintenance records were reviewed:
Fire alarm as of 05.01.2015
Health and safety risk assessment as of 27.11.2014
Facilities Risk assessment
Pat testing as of 01.09.2014
Annual service for extinguishers as of 11.05.2015
Electrical installation condition report as of 08.06.2014
Periodic inspection report as of 20.04.11
UPS maintenance log as of 10.09.2014

The following exceptions were noted:

During the visit in the Fitness to Practise two unattended working stations were noted without applying screen lock as per Policy requirements A11.2.9 Tidy Desk Policy/1.1/28.04.2015 / 5.3 "All devices including mobiles laptops should be locked when not in use" & 7.15 "If you intend to leave any computer switched on and unattended in the office at any you must lock your computer screen". See minor NC raised below.

Maintenance records were made available at the time of the assessment. The guide confirmed that the Facilities Manager was not on site and facilities staff could not provide the records. Maintenance records dated 28/01/2015 for air condition were sampled.

Cabling in server room was seen to be in an untidy manner. See observation raised below.

# Observations.

| Type | Area/Process | Clause |
|---|---|---|
| Observations | Physical Security | A11.2.3 |
| Scope | IS 600771 | |
| Details: | Cabling in the server room was seen to be in an untidy manner. | |

| Type | Area/Process | Clause |
|---|---|---|
| Observations | Physical Security | 7.5.3 |
| Scope | IS 600771 | |
| Details: | Maintenance records should be available and stored within departmental shared folders for ease of access. This will avoid situations of not being able to produce the requested information on time due to unavailability of the Facilities Manager as an example. | |

**Human Resource : 7, A.7**

IS training takes place through the induction process and refresher courses take place on an annual basis. There is an on-line training academy as well. An IS competition has been recently launched in the company's website and the completion date is due for 22/05/2015. The training material in the "New Employees and Contractor Pack" was reviewed and the questionnaire had 80% passmark. In addition the IS questionnaire in service monkey was reviewed. The employees training log was reviewed. There is a 10% of employees who have not passed successfully the course and notifications have been send.

In the company's intranet there is a board listing IS news, events and recent updates. Policies and documented procedures are included in the intranet.

Skills - Knowledge and Abilities are included in the employees job roles. Confidentiality terms, data protection and handling, disciplinary and grievance terms are included in the employment contract. In addition the employees hand book includes the IT Policy, Data Handling guidance, e-mail guidance, HR procedures, Disciplinary procedures etc. Employees sign off the IT Policy.

Competency records of the IS Auditor were seen to be in place.

Screening process takes place via verification of qualifications, 2 references at minimum and CRBs (role based).
Sample seen: Hearings Officer as of 08/09/2015. An employee checklist was seen to be attached on the records.

In leavers procedure a notification letter is sent to the employee for returning the company's items and a file is raised in the Recruitment and employees change database as per process seen above under sec.A.9
Sample seen: Case Manager as of 21/05.2015

**Awareness : A.7.2.2**

Awareness sessions took place in the following departments:
Policy and Standards / policy officers (including new starter), Fitness to Practise / Investigations Manager Case Manager, Schedule Managers, , Compliance Officers, Registrations / Head of Registrations, Registrations Manager, Registrations Leader, member of staff (new starter) and the Secretariat.

Interviews took place with top management and staff. Good levels of awareness were demonstrated in the following areas:
Policies and procedures
Policy officers
Tidy Desk Policy
Secure handling of information
Secure handling of equipment
Passwords policy and application to Computers, Laptops, mobile devices
Secure use and disposal of documents
Secure disposal of information (including e-mails)
Secure communication of e-mails via password protected documents (passwords sent by separate e-mail), bcc.
Bob's training
Induction training
IS training
Encrypted memory sticks
Secure log in procedures
Reporting incidents and breaches
IS Objectives
Risks around processes and how to communicate them
Resourcing and forecast

Access control
IS Policy
IS Completion
IS Survey Monkey Questionnaire

**Closing Meeting :**

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

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

# Minor Nonconformities Raised at Last Assessment.

| Ref | Area/Process | Clause |
|---|---|---|
| 1174100N1 | Management System, Policies and Objectives, Documented Information Organisational Planning and Control | 6.2 |
| Scope | IS 600771 | |
| Details: | Information security requirements not fully met | |
| Requirements: | Information security objectives and planning to achieve them<br>The organization shall establish information security objectives at relevant functions and levels.<br>The information security objectives shall:<br>a) be consistent with the information security policy;<br>b) be measurable (if practicable);<br>c) take into account applicable information security requirements, and results from risk assessment and risk treatment;<br>d) be communicated; and<br>e) be updated as appropriate.<br>The organization shall retain documented information on the information security objectives.<br>When planning how to achieve its information security objectives, the organization shall determine:<br>f) what will be done;<br>g) what resources will be required;<br>h) who will be responsible;<br>i) when it will be completed; and<br>j) how the results will be evaluated. | |
| Objective Evidence: | The Information Security Objectives reviewed was silent on who will be responsible for achieving the objectives set. The objectives reviewed had some metrics (for those that were measureable), but it was difficult to ascertain whose responsibility it was to achieve the objectives as listed. HCPC must ensure that the requirements of clause 6.2 are fully met, especially 6.2i. | |
| Actions: | Confirmed. Information Security Objectives set out within Doc A3 Effectiveness Measures issued on 02/04/2015 showed all the metrics, timeline as well as those responsible for achieving the objectives. | |
| Closed?: | Yes | |

# Minor Nonconformities Arising from this Assessment.

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

| Ref | Area/Process | Clause |
|---|---|---|
| 1193099N2 | Physical Security | A11.2.9 |
| Scope | IS 600771 | |
| Details: | The Tidy Desk Policy/1.1/28.04.2015 was not seen to have been effectively implemented. | |
| Requirements: | Clear desk and clear screen policy<br>A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted. | |
| Objective Evidence: | During the visit to Fitness to Practise two unattended working stations were noted without applying screen lock as per Policy requirements A11.2.9 Tidy Desk Policy/1.1/28.04.2015 / 5.3 "All devices including mobiles laptops should be locked when not in use" & 7.15 "If you intend to leave any computer switched on and unattended in the office at any time you must lock your computer screen". | |

# Assessment Participants.

On behalf of the organisation:

| Name | Position |
|---|---|
| Roy Dunn | Head of Business Process Improvement |
| Marc Seale | CEO/Registrar |
| Greg Ross-Sampson | Director of Operations |
| Kayleigh Birtwistle | Quality Compliance Auditor |
| Richard Campo | Information Security Consultant (ITG) |
| Guy Gaskins | IT Director |
| Claire Reed | Project Portfolio Manager |
| Claire Amor | Information Governance Manager |
| Rick Welsby | IT Support Manager |
| Kim Wilcox | HR Advisor |
| Simon Thompson | Case Manager, FTP |
| Andrew Gillies | Finance Director |
| Chantelle Mayoss | Transaction Manager |
| Charlotte Avery | Head of Financial Accounting |
| Zoe Yankson | Purchase Ledger Officer |
| Jacqueline Ladds | Communication Director |
| Robyn Schnuir | Project Manager |
| Tony Glazier | Web & Digital Manager |
| Steven Nicol | Web & Digital Officer |
| Brendon Edmonds | Head of Educational Development |
| Alan Shilabeer | FTP – Investigations Manager |

The assessment was conducted on behalf of BSI by:

| Name | Position |
|---|---|
| Evangelia Arfara | Team Member |
| Kwadwo Anim-Appiah | Team Leader |

# Continuing Assessment.

BSI believes in a partnership approach that provides added value service. It is on this basis that we propose a programme of continuing assessment as detailed below.

| Site Address | Certificate Reference/Visit Cycle | |
|---|---|---|
| Health & Care Professions Council<br>Park House<br>184 Kennington Park Road<br>London<br>SE11 4BU<br>United Kingdom | Certificate reference to be advised | |
| | Visit interval: | 12 months |
| | Visit duration: | 2 Days |
| | Next re-certification: | 01/04/2018 |

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

# Certification Assessment Plan.

HEALTH-0047125084-000|IS 600771

| Business area/Location | | Visit 1 | Visit 2 | Visit 3 | Visit 4 | Visit 5 | Visit 6 |
|---|---|---|---|---|---|---|---|
| | 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 and Access Control | | | 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 | |
| Risk Assessment, Risk Treatment, Statement of Applicability | | X | X | X | X | X | |
| Compliance: Legal and Other Requirements | | X | X | | | X | |
| Security Incident Management | | X | X | X | X | X | |
| Communications | | X | X | | | X | |
| Physical and Environmental Security | | 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 | |
| Programme Management (additional 1 day to review the next 3 year cycle) | | | | | | | X |

# Next Visit Plan.

**Visit objectives:**

**CAV**

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

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

| Date | Assessor | Time | Area/Process – Day 1 | Clause |
|---|---|---|---|---|
| 13/04/2016 | Kwadwo Anim-Appiah | 9:00 | Opening Meeting including changes to the management system | |
| | | 9:15 | Performance Monitoring & Measurement / ISMS Objectives | 9.1, 6.2 |
| | | 9:45 | ISMS Monitoring and Improvement; Internal Audit; Management Review; Corrective Action / | 9.2, 9.3, 10 |
| | | 10:45 | Incident Management | A.16 |
| | | 11:45 | Risk Management & Risk Treatment | 6 |
| | | 12:45 | Lunch | |
| | | 13:45 | Business Continuity | A.17 |
| | | 15:15 | Report Write-up (offsite) | |
| **Date** | **Assessor** | **Time** | **Area/Process – Day 2** | **Clause** |
| 14/04/2016 | Kwadwo Anim-Appiah | 9:00 | Update Meeting | |
| | | 9:15 | Operations Security (IT Department) | A.12 |
| | | 10:15 | HR Security | A.7 |
| | | 11:15 | Fitness to Practise (Awareness Sampling) | A.7.2.2 |
| | | 12:00 | Registrations (Awareness Sampling) | A.7.2.2 |
| | | 12:30 | Lunch | |
| | | 13:30 | Facilities (Awareness Sampling) | A.7.2.2 |
| | | 14:45 | Report Preparation | |
| | | 16:30 | Closing Meeting | |

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

# Notes.

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

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

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

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

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

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

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

Tel: +44 (0)845 080 9000 Fax +44 (0)1908 228123

Email: MK.Customerservices@bsigroup.com