HCPC's Risk Assurance Part 1

ISO & Assurance

Audit Committee

14 June 2017

Three pronged approach

BSI / NAO / Commercial Internal Audit

Departmental controls, "in dept" QA effort

BPI ISO9001, ISO27001, ISO10002; Near Miss Reporting
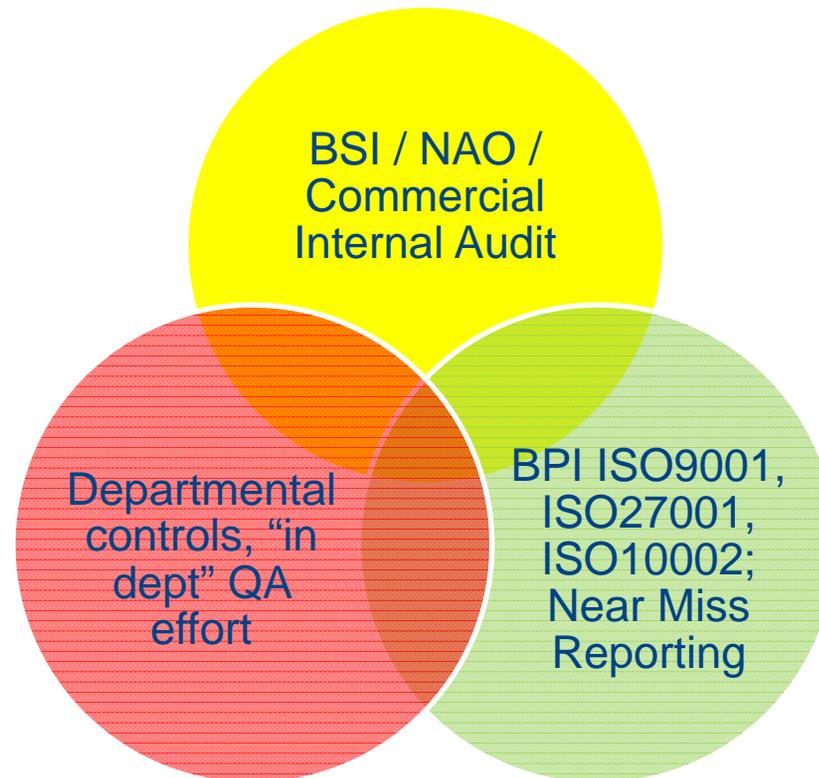
Summary Non ISO Standards based audit and assurance

Financial Matters

Grant Thornton, Mazars, PKF

Governance

NAO

Regulatory matters

PSA
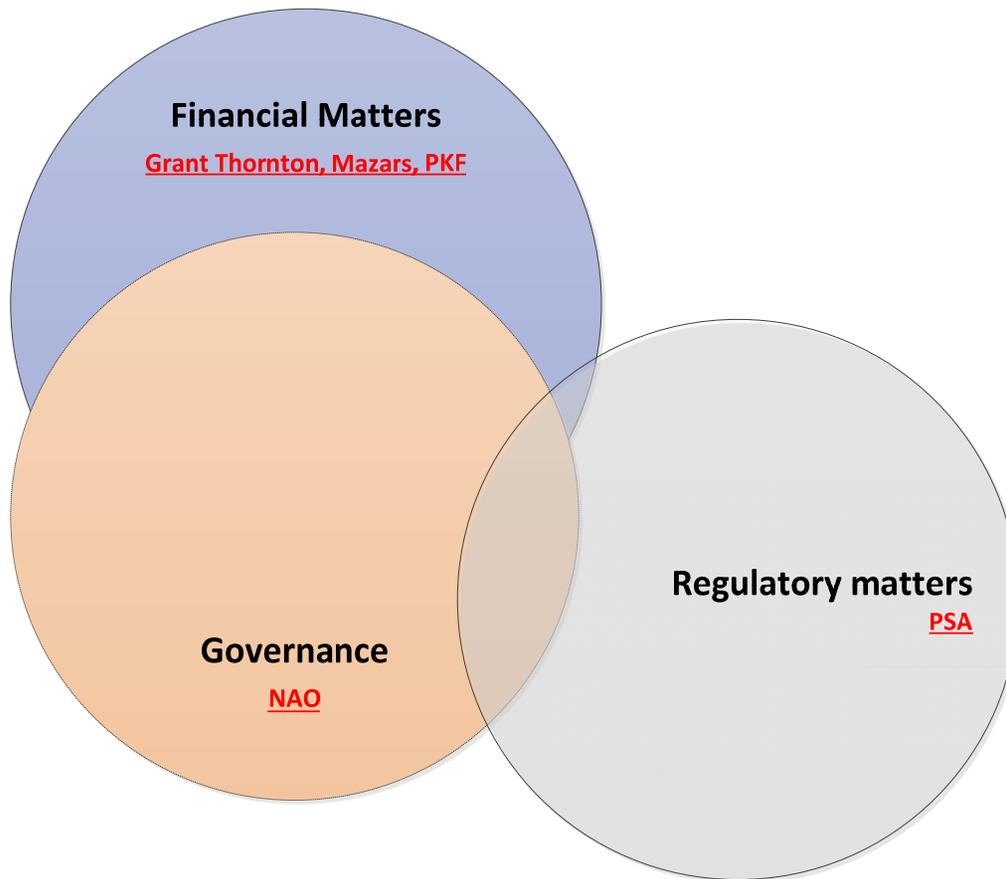
Summary of HCPC ISO standards used

- ISO9001 [a system where all the management processes are linked up, with a risk or continuous improvement approach, eg link between workload, predicted workload, resources, risk and remediation of process or system failures; across the whole organisation]

- ISO27001 [information security of data, processes, systems and people, risk based]

- ISO10002 [complaints management / customer service as a mechanism of capturing what is going wrong and getting issues assessed for corrective action] Reliant on stakeholder feedback. Cannot rely on feedback here warning us of issues.

Which ISO standards do we use for Assurance?

ISO 9001 Quality Assurance

ISO 27001 Information Security

Risk Assurance Map

ISO standards are one of the 16 types of assurance mechanism

Key Business Risk areas Assurance Map	Systems Controls	Operational Risk Management	Inter-departmental Quality Assurance	Near Miss Reporting	EMT	Council	Audit Committee	Internal Auditors	External Auditors (NAO)	External Legal Advice	Quality Management System ISO9001	Information Security Management ISO27001	PSA	Penetration Testing	PCI-DSS	Parliamentary oversight
	AREA C. Management Control & Reporting				**AREA B.** Functional oversight / Governance	**AREA A.** Independent review / Assurance / Regulatory oversight										
Strategic risks						x	x	x		x						x
Communications		x	x	x	x	x	x	x	x	x	x		x			
Continuing Professional Development	x	x	x	x	x		x			x						
Corporate Governance			x	x	x	x	x	x	x	x	x		x			x
Information Security	x	x	x	x	x		x	x			x	x		x	x	
Education	x	x	x	x	x	x	x	x		x	x		x			
Finance	x	x	x	x	x	x	x	x	x	x	x	x			x	x
Fitness to Practise	x	x	x	x	x	x	x	x		x	x		x			x
HR	x	x	x	x	x	x	x	x		x	x	x				
Information Technology	x	x	x	x	x	x	x	x	x	x	x	x		x		
Legal			x	x	x	x	x	x		x			x			x
Operations	x	x	x	x	x	x	x	x	x		x		x			
Partner	x	x	x	x	x	x	x	x			x	x	x			
Pensions			x	x	x	x	x	x		x						
Policy & Standards			x	x	x	x	x	x		x	x		x			x
Project Management	x	x	x	x	x	x	x	x	x		x	x				
Quality Management	x	x	x	x	x	x	x	x			x		x			
Registration	x	x	x	x	x	x	x	x		x	x		x			

What is ISO9001?

An internationally recognised standards that covers quality, consistency and improvement across an organisation. Management System

Authority
Responsibility
Accountability
Planning
Change

Process Owner

Correction
Improvement
Amendments

Change ?

Measure

Product
Process

Key activities

Input

Output

Statement of requirements

Deliverables
- Hardware
- Software
- Processed material
- Service

Resources

Criteria

Records

Human resource
Environment
Tools
Equipment
Materials
Communications
Utilities
Services
Other

Legislative
Regulatory
Customer
Corporate
Standards
Procedures

Compliance
Status
Position
Authorisation

Take some inputs, apply some resources to them via a process, to create the required outputs.

Simple process example

What is a process?

Example process – making the tea

INPUTS	Apply some resources	OUTPUTS

What does that mean in real language?

Water	Boil some water
Heat	Place in pot
Tea	Add tea (bags or leaves)
Milk	Stew!
Sugar	Pour into cups or mugs
	Add milk and sugar as required

ISO 9001 Standards – benefits of the core requirements

- All processes mapped

- Processes are auditable and measureable

- Audits test the accuracy of processes, offering opportunity for continual improvement

- Risk based or process based audits

- Senior Management Responsibility [EMT]

- Linking strategy to risk; risk to departmental work plans; work plans to budget. This is the only place this happens.

- Resource management based on prediction of work levels (Registrant forecast feeds HR & Financial requirements)

- Document control – we are using the right version

- ISO9001 over time;

    - 9001:2000 = follow the process;

    - 9001:2008 = "Continuous Improvement";

    - 9001:2015 = "Risk based".

Other ISO standard benefits

Plan, Do, Check, Act cycle – ensuring we continually improve

Design it; Run it; Audit it; Fix it. Start again.

Sample process
Statutory Regulation – Process for Introduction

Statutory Regulation – Process for Introduction

	Consider and assess suitability	Publish and refine proposals	Approve and publish Legislation, Rules & Standards	Transfer Register	Grandparenting	Post GP
Government	Consider Statutory Regulation → Assessment (Political) → Decision to develop proposals (Reject)	Policy Proposal / Draft Legislation / Regulatory Impact Assessment → Consult → Decision to Statutory Regulate (Reject)	Parliamentary Approval of Legislation • Protected Title • Register to Transfer • GP Window • Approved programmes (Reject) → Publish Legislation			
Regulator	Consider statutory regulation → Assessment (Technical) → Recommend profession for statutory regulation		Draft Rules / Draft Standards / Identification of data / Government grant → Consult → Publish Rules & Standards / Communication		Open Register → Collect fees / Transfered FTP cases / Visit programmes	Start CPD portfolio auditing
Non Statutory Regulated profession	**Body of knowledge** Discrete area of activity / Displays some homogeneity / Evidence of efficacy	**Profession** Attributes of profession and Degree of Establishment	**Established professional body** Voluntary Register / Defined routes to entry / Independently assessed entry qualifications / Standards of Conduct Performance & Ethics / FTP process / Continuing Professional Development	Voluntary Register / Education programmes / FTP files	Registrants collect CPD information	

Health & Care Professions Council

ISO 9001 Standard in action

| Internal Audit | DEPT | EMT Assess Proposed change | Process update | Re-audit in cycle |

Worked example – Partner appraisal / assessment process

| Predicted resource shortfall | Time & Motion study & workload model | Proposal and approval of extra resource | Additional resource added to the process | Fully functioning process |
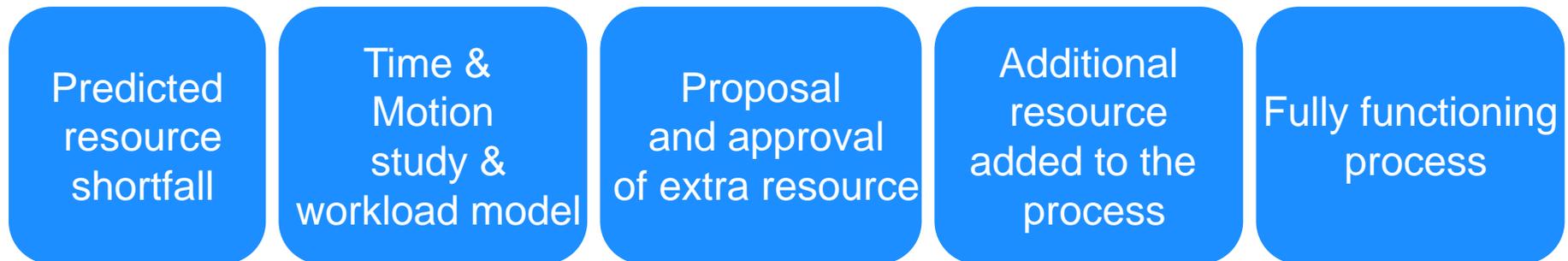
ISO27001:2013 Information Security

- Build and maintain a list of Information assets, and monitor the vulnerabilities and threats to them

- Regular audits – Tidy Desk, across the whole organisation, unannounced

- "Kicking the tyres" Shoving the doors, Penetration Testing (IT Dept)

- All Business Continuity / Disaster Recovery events audited/reported

- Employees, Partners and Council Members trained on an annual basis

- Customer property (= applicant/registrant/witness/stakeholder data) in ISO 9001 is protected

Item	Asset	Impact - confidenti ality	Impact - integrity	Impact - availab ility	Risk	Confid entialit y	Integri ty	Availab ility	Likelih ood - confid entiali	Likelih ood - integr ty	Likelih ood - availab ility	Risk rating - confid entiali	Risk rating - integr ty	Risk rating - availab ility	Control	Control referen ce	Residu al risk rating confi	Residu al risk rating integ	Residu al risk rating avail	Status
75	NetRegulate exported print files	5			Compromise of information: Disclosure due to Organization: Lack of procedure of monitoring of information processing	Yes	n/a	n/a	2			10			Addressing security within supplier agreements	A.15.1.2	3			OK
76	NetRegulate exported print files	5			Compromise of information: Disclosure due to Organization: Lack of procedure of monitoring of information processing	Yes	n/a	n/a	2			10			Monitoring and review of supplier services	A.15.2.1	3			OK
77	NetRegulate exported print files		3		Unauthorised actions: Corruption of data due to Software: Lack of audit trail	n/a	Yes	n/a		2			6		Protection of log information	A.12.4.2		6		OK
78	NetRegulate exported print files		3		Unauthorised actions: Corruption of data due to Personnel: Lack of monitoring mechanisms	n/a	Yes	n/a		2			6		Protection of records	A.18.1.3		6		OK

Sample ISO27001 process, part of Incident Management

health & care professions council

BPI-INCIDENT MANAGEMENT PROCESS & RESPONSIBILITIES – Information Security

Phase

| INCIDENT DETECTED by business, stakeholder or other | Incident alerted to **informationsecurity@hcpc-uk.org** (telephone + email details) Or verbally to Information Governance Manager, Head of BPI, or an EMT Member → Chief Executive & Registrar notified / Acting Chief Executive notified |

Decision on nature and reaction required to reported incident

Initial assessment of incident and log against a Risk matrix by primary Information Governance or Information Security role. See over → Take appropriate action determined by Risk i.e. escalate or close (alert IT to take corrective or/and protective action, alert Secretariat for DPC, alert business team manager involved etc) → Refer to Data **Incident Risk Rating Procedure (Assessment matrix)** Assess impact of incident

Reaction to incident, minimisation of impact

Convene an emergency meeting of the Information Security group (to take coordinated action where a high risk) else review on a regular and periodic Information Security group meeting.

Information Security Group consists of;
- Chief Executive & Registrar
- Director of Operations (*Risk*)
- Director of Information Technology
- Information Governance Mgr or Director of Council & Committee Services (DPA & FOI compliance)
- Head of Business Process Improvement (*information security*)

All on circulation list of informationsecurity@hcpc-uk.org
Members of Executive Management Team as available

Post incident closure and reporting

- Complete a post incident report and review at to the period information security group who escalate for information as appropriate to Council.
- Report incident to ICO and or PSA as required

ISO 27001 Standard in action

hcpc health & care professions council

| Internal Audit | BPI create New policy | EMT Assess Proposed change | Implement and promote new policy | Re-audit in cycle |

Worked example – information stored on desks

| Clear Desk Policy in operation | Low level breaches of Clear Desk Policy with no information risk | Proposal to revise process to Tidy Desk Policy | Tidy desk - more pragmatic approach. | Fully functioning policy |

Why ISO 27001 if we have ISO9001?

- An international standard on information security, that is not sector specific

- Independently audited

- Ensures continuous improvement in security

- Ensures we have an up to date information asset list with associated risk ratings around confidentiality, integrity and availability

- A set of off the shelf controls (mitigations) that must be explicitly accepted or rejected with reasons, and are recorded in the Statement of Applicability

- 114 controls in 14 groups and 35 control objectives

- Although management systems elements are included, (as in ISO9001) the ISO27001 standard includes an opt in / opt out shopping list of security activities, that must be selected or not selected with recorded reasoning

BPI activity in numbers

hcpc health & care professions council

360 processes
ISO9001;
27001; 10002

44 Internal
Audit event areas

10-30 updates to the QMS,
ISMS, CMS per year. All ISMS
Policy documents refreshed

13 departments
internally audited
plus Near Misses

Unannounced
Tidy Desk &
Information security
audits as required

BSI external audits
4 days ISO9001 pa,
2 days ISO27001 pa,
2 days ISO10002 pa

Information Security
training
250+ employees
Trained
650 partners trained

2 Risk Register updates;
Registrant forecasts;
BCM/DR tests;

+ Major projects, delivering
new sets of processes
for depts, requiring update of
the QMS/ISMS

HCPC's relative audit effort

Relative effort and overlap of Quality Assurance / Audit activity, internal vs. external systems
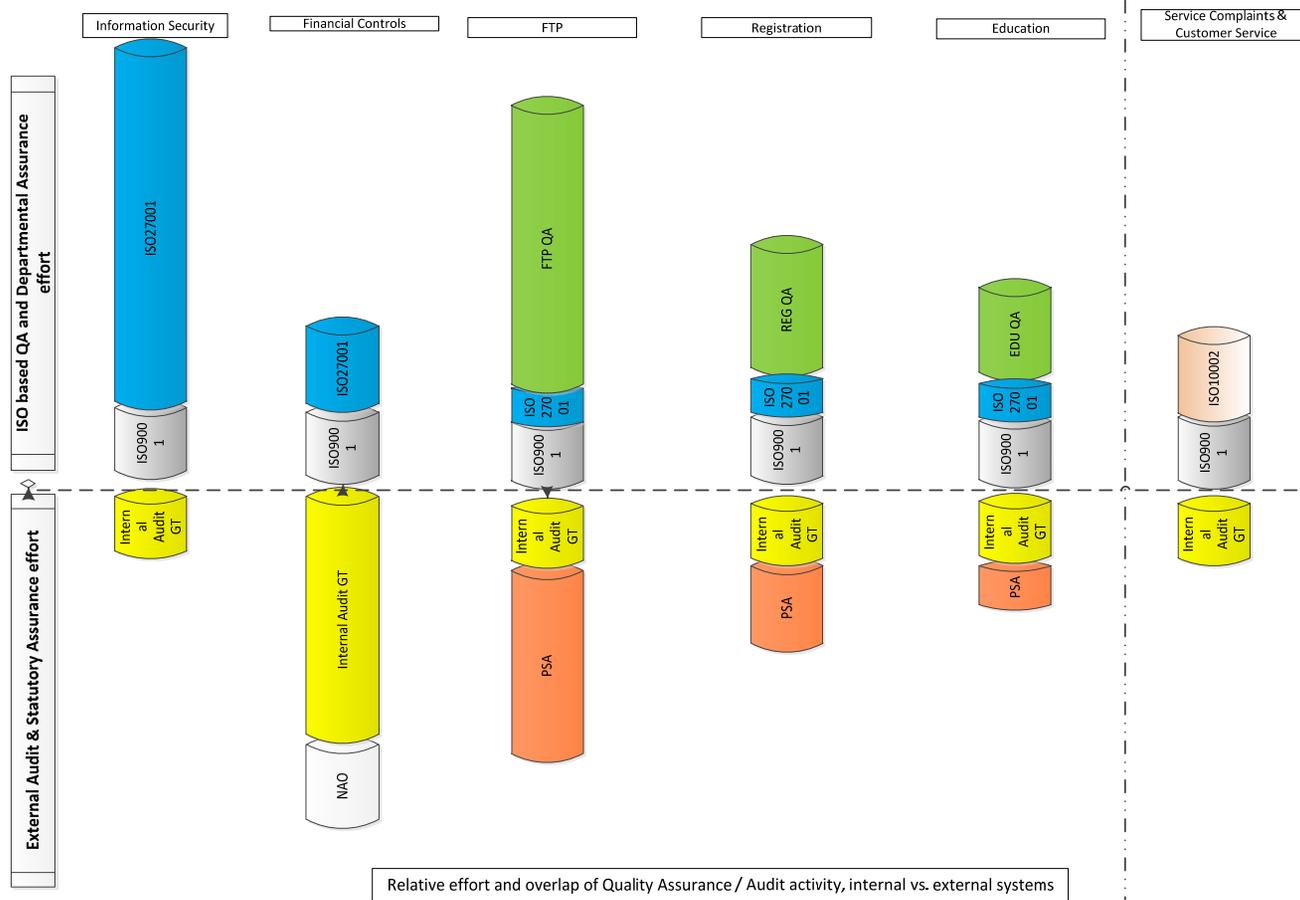
Key

BSI & BPI ISO27001 based audit	BSI & BPI ISO10002 based audit	National Audit Office (statutory requirement)
Internal Audit function	BSI & BPI ISO9001 based audit	
Departmental QA	Professional Standards Agency	

HCPC's audit across all departments

Very approximate audit effort in each HCPC area by auditor group.

PSA

| Chief Exec & Secretariat | Communications | Education | Policy and Standards | Ops/ Registrations | Fitness to Practise | Office Services | Finance | Partners | Human Resources | IT | Projects |

HCPC's internal assurance effort by internal department teams

Continual business improvement by Assurance

External quality assurance

Internal departmental quality assurance

ISO9001 & ISO27001 & ISO10002; external to depts (BPI audit QMS/ISMS), including certification body audits (BSI)

Commercial Audit Function – Mazars, Grant Thornton, PKF

FTP

A&D team x 7

Case team Managers

Case Managers

REG

QA Mgr, QA officer

Reg managers Reg Team leaders

Reg advisors

EDU

Quality Team x4

Education Managers

Education Officers

Independent Internal assurance

Departmental assurance activity

Managers

Employees

HCPC's QMS – processes in ISO9001

Information Security ISO27001:2013

THE HEALTH AND SOCIAL WORK PROFESSIONS ORDER 2001.
THE HEALTH AND SOCIAL CARE ACT 2012

Stakeholders

Privy Council

Governance

Council

Plan

Secretariat & Customer Service

Public

Communications

Fitness to Practise

Policy & Standards

Education

Safeguard Health and Well-being of Users

Registrants (Practitioners)

Users of Registered Practitioners

Executive Management Team

Cross Directorate Team

Act

Do

Public

Registrations

Operations

- Quality / Information Security & DR / Risk / Business Process Improvement / InfortionServices - Reporting
-
- Project Management
- Facilities
- Finance
- Human Resources
- Information Technology

Support Services

Unexpected persons or packages in secure areas – what to do.

Check

ISO9001:2015 Quality management systems

PLAN	DO	CHECK	ACT

4. Context of the organisation → **5.Leadership** → **6.Planning** → **7.Support** → **8.Operation** → **9.Performance evaluation** → **10. Improvement**

4. Context of the organisation
- 4.1 Understanding the organisation and its context
- 4.2 Understanding the needs and expectations of interested parties
- 4.3 Determining the Scope of the QMS
- 4.4 Quality Management System and its processes

5.Leadership
- 5.1 Leadership & commitment
- 5.2 Policy (Quality policy)
- 5.3 Organizational roles, responsibilities & authorities

6.Planning
- 6.1 Actions to address risks & opportunities
- 6.2 Quality objectives & planning to achieve them
- 6.3 Planning of changes

7.Support
- 7.1 Resources
- 7.2 Competence
- 7.3 Awareness
- 7.4 Communication
- 7.5 Documented information

8.Operation
- 8.1 Operational planning & control
- 8.2 Requirements for products & services
- 8.3 Design & development of products & services
- 8.4 Control of external provision of goods & services
- 8.5 Production and service provision
- 8.6 Release of products & services
- 8.7 Nonconforming products & services

9.Performance evaluation
- 9.1 Monitoring, measurement, analysis & evaluation
- 9.2 Internal audit
- 9.3 Management review

10. Improvement
- 10.1 General
- 10.2 Nonconformity & corrective action
- 10.3 Continual Improvement

20150925 ISO9001:2015 structure

ISO27001:2013 Information security management systems

ISO27001:2013 standard for Information Security

Section 5: Information security policies

- 5.1 Management direction for information security

Section 6: Organization of information security

- 6.1 Internal organization
- 6.2 Mobile devices and teleworking

Section 7: Human resource security

- 7.1 Prior to employment
- 7.2 During employment
- 7.3 Termination and change of employment

Section 8: Asset management

- 8.1 Responsibility for assets
- 8.2 Information classification
- 8.3 Media handling

Section 9: Access control

- 9.1 Business requirements of access control
- 9.2 User access management
- 9.3 User responsibilities
- 9.4 System and application access control

Section 10: Cryptography

- 10.1 Cryptographic controls

Section 11: Physical and environmental security

- 11.1 Secure areas
- 11.2 Equipment

Section 12: Operations security

- 12.1 Operational procedures and responsibilities
- 12.2 Protection from malware
- 12.3 Backup
- 12.4 Logging and monitoring
- 12.5 Control of operational software
- 12.6 Technical vulnerability management
- 12.7 Information systems audit considerations

Section 13: Communications security

- 13.1 Network security management
- 13.2 Information transfer

Section 14: System acquisition, development and maintenance

- 14.1 Security requirements of information systems
- 14.2 Security in development and support processes
- 14.3 Test data

Section 15: Supplier relationships

- 15.1 Information security in supplier relationships
- 15.2 Supplier service delivery management

Section 16: Information security incident management

- 16.1 Management of information security incidents and improvements

Section 17: Information security aspects of business continuity management

- 17.1 Information security continuity
- 17.2 Redundancies

Section 18: Compliance

- 18.1 Compliance with legal and contractual requirements
- 18.2 Information security reviews

ISO 27001 operates on the processes used in ISO 9001 activities

HCPC's Management Review summary

HCPC's Improvement Log – output for HCPC QA framework

Ref No. BPWGM	Incident Date	Date Logged	Raised By	Type	Description of Finding/Issue BPWGM/Internal Auditor	Root cause, N/A if no Observations or NC's found in audit BPWGM/Internal Auditor	MANAGEMENT RESPONSE	Corrective and/or Preventive action planned/taken	Risk Rating = Impact x Likelihood 10 to 25 = High = Red 6 to 9 = Medium = Yellow 1 to 5 = Low = Green	DEPT/ DIRECTORATE	Responsible person ASSIGNED by EMT	Target date EMT AGREED	Action taken EMT REPORTED	effectiveness EMT FEEDBACK to Internal Auditors BPWGM etc	ISSUE Closed?	Date closed	NCN Closed
REC HS2 internal audit report Comms-Stakeholders MAR2016	01/03/2016	01/03/2016	Hd of BPI	IA	Issues Brief process now uses Dot.Mailer for bulk email campaigns. Update to ISO9001 process in Stakeholders comms required	QM not informed when change over occurred	Process updated		1		Stakeholder Comms Mgr	01/03/2016	process updated	######	Y		
ITG201603-NC1	42432	03/03/2016	ITGov	IS	A8.3.2 – Disposal of media. Information in confidential bins was overflowing and accessible (seen across a number of departments); management should review the effectiveness/frequency of confidential waste disposal.	Some bins in 405 KR not emptied; some documents not pushed through opening completely and were thus retrievable.	Depts requested to inform Facilites if bins full or not emptied on time. Depts to ensure docs pushed completel into the bins, watch out for visitors using bins incorrectly	12		Facilities & Depts	05/03/2016	Additional bins added and employees advised to contact Facilities if bins are full to ensure they're emptied	Seems as though collections aren't happening weekly and will discuss with Facilities 30/03/2016	Ongoing		

A report reference number, linking back to the original NMR, Internal Audit etc

A description of the problem or issue

What is going to be done to address it.

What has been done to address it.

To enable protection of the public and deliver continuous improvement

- **Proportionate**
- **Collaborative / inclusive**
- **Auditor independent of process**
- **Common measures where possible**
- **Evidence based**
- **Reproducible**
- **Reflecting ISO standards where possible**
- **Risk based vs. reactionary (as required)**
- **Timeliness of remediation**
- **Incorporating stakeholder feedback**
- **Specifically targeted vs. non targeted (as required)**
- **Monitored timeliness and completeness**

- **Independent of performance management**

Proportionate levels of reporting upwards and within functions or departments

Reflecting on effectiveness of QA effort

Any Questions? Another session required?

?