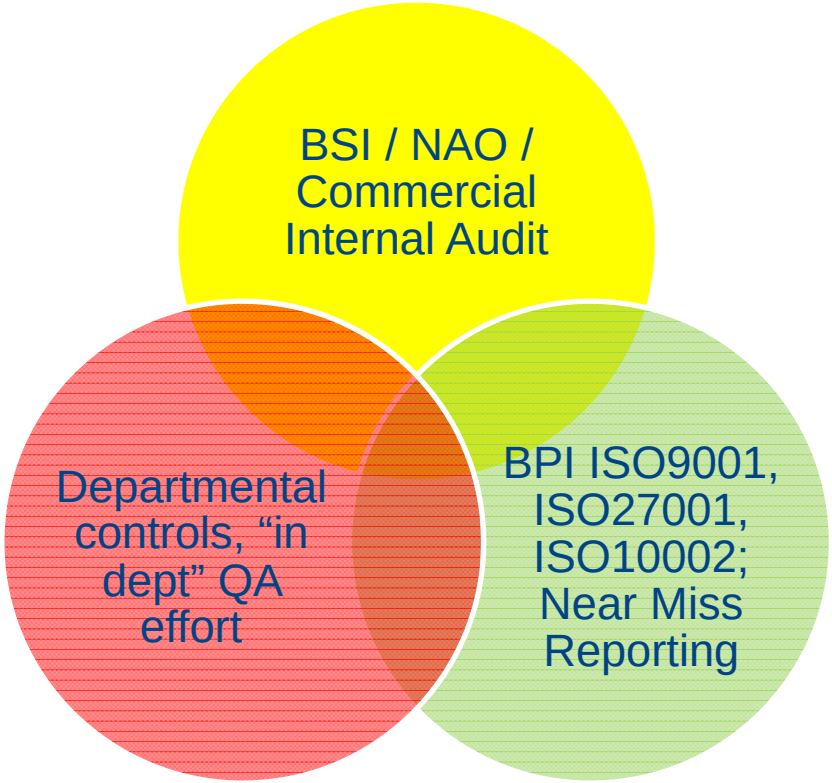
HCPC's Risk Assurance Part 1

ISO & Assurance

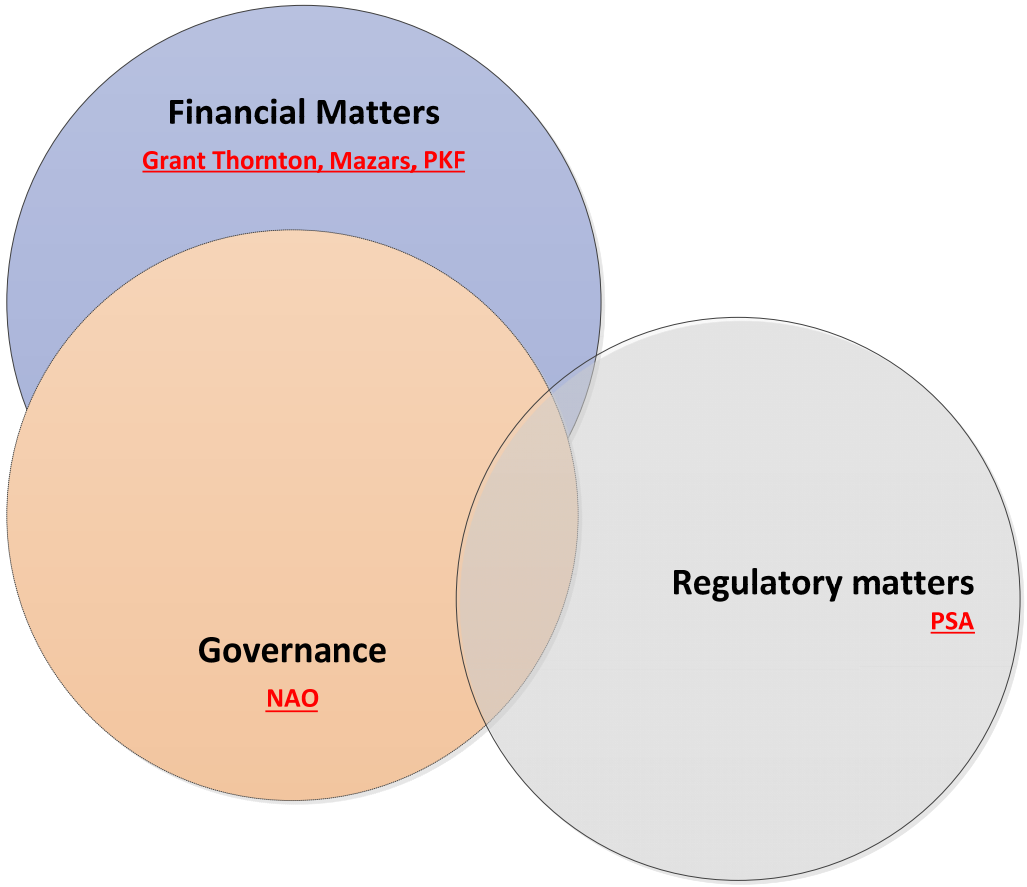
Audit Committee

14 June 2017

Three pronged approach



Summary Non ISO Standards based audit and assurance



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

bsi.

Certificate of Registration

QUALITY MANAGEMENT SYSTEM - ISO 9001:2008

This is to certify that: Health & Care Professions Council
Park House
184 Kennington Park Road
London
SE11 4BU
United Kingdom

Holds Certificate Number: FS 83074

and operates a Quality Management System which complies with the requirements of ISO 9001:2008 for the following scope:

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

For and on behalf of BSI:

Gary Fenton, Global Assurance Director

Originally registered: 13/07/2004 Latest Issue: 17/06/2013 Expiry Date: 01/07/2016

Page: 1 of 1

...making excellence a habit.

This certificate was issued electronically and remains the property of BSI and is bound by the conditions of contract.
An electronic certificate can be authenticated online.
Printed copies can be validated at www.bsigroup.com/ClientDirectory

Information and Contact: BSI, Kitemark Court, Davy Avenue, Knowlhill, Milton Keynes MK5 8PP. Tel: + 44 845 080 9000
BSI Assurance UK Limited, registered in England under number 7805321 at 389 Chiswick High Road, London W4 4AL, UK.
A Member of the BSI Group of Companies.

ISO 27001 Information Security

bsi.

By Royal Charter

Certificate of Registration

INFORMATION SECURITY MANAGEMENT SYSTEM - ISO/IEC 27001:2013

This is to certify that: Health & Care Professions Council
Park House
184 Kennington Park Road
London
SE11 4BU
United Kingdom

Holds Certificate Number: IS 600771

and operates an Information Security Management System which complies with the requirements of ISO/IEC 27001:2013 for the following scope:

The management and operation of the Health & Care Professions Council (HCPC) covering statutory professional self-regulation, and reports to the Privy Council. This is in accordance with the Statement of Applicability version 1.2 dated May 2015.

For and on behalf of BSI:

Frank Lee, EMEA Compliance & Risk Director

Original Registration Date: 12/06/2015 Effective Date: 12/06/2015
Latest Revision Date: 12/06/2015 Expiry Date: 11/06/2018

Page: 1 of 2

...making excellence a habit.

This certificate was issued electronically and remains the property of BSI and is bound by the conditions of contract.
An electronic certificate can be authenticated online.
Printed copies can be validated at www.bsigroup.com/ClientDirectory

Information and Contact: BSI, Kitemark Court, Davy Avenue, Knowlhill, Milton Keynes MK5 8PP. Tel: + 44 845 080 9000
BSI Assurance UK Limited, registered in England under number 7805321 at 389 Chiswick High Road, London W4 4AL, UK.
A Member of the BSI Group of Companies.

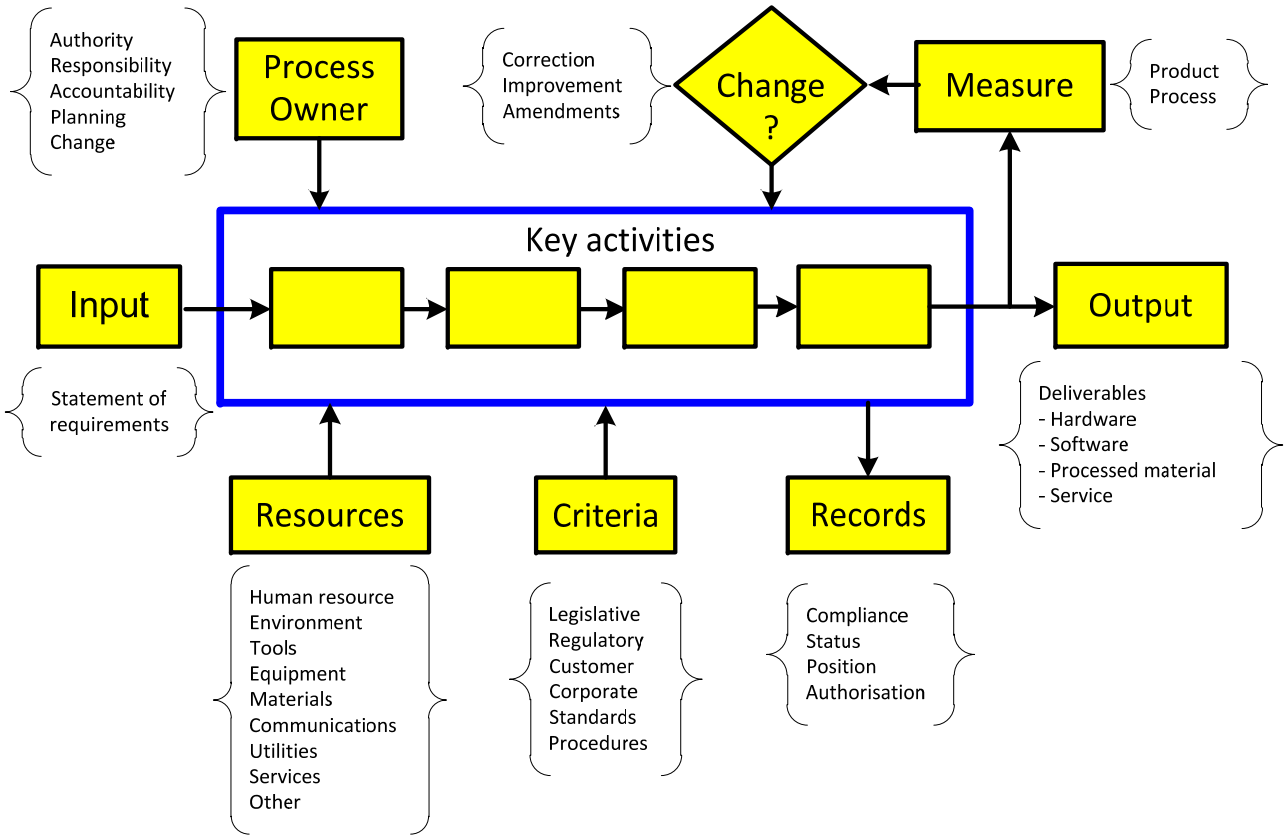
Risk Assurance Map

ISO standards are one of the 16 types of assurance mechanism

	AREA C. Management Control & Reporting				AREA B. Functional oversight / Governance	AREA A. Independent review / Assurance / Regulatory oversight											
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
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
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							
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



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?

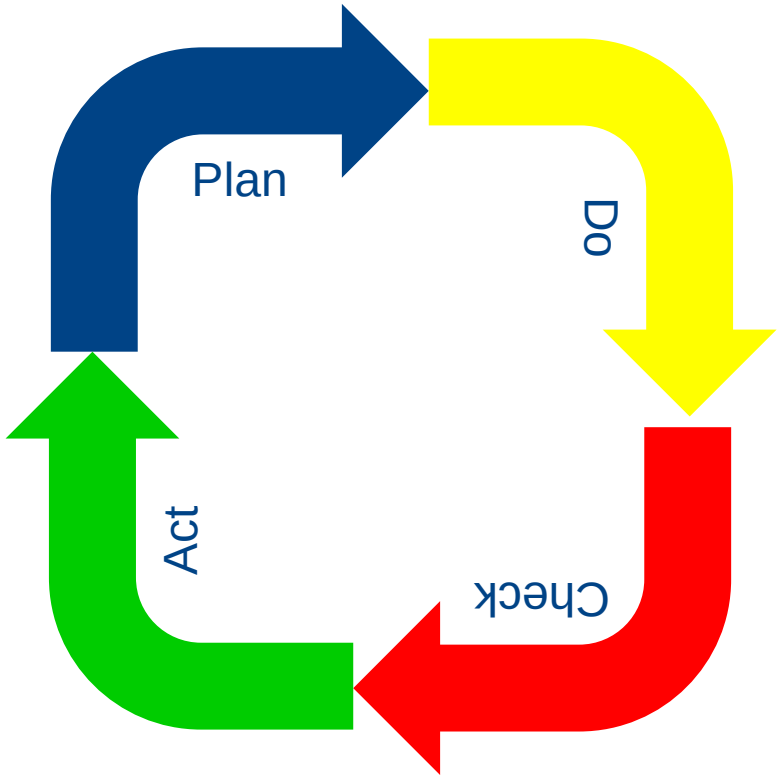
Water	Boil some water
Heat	Place in pot
Tea	Add tea (bags or leaves)
Milk	Stew!
Sugar	Pour into cups or mugs
	Add milk and sugar as required

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”.

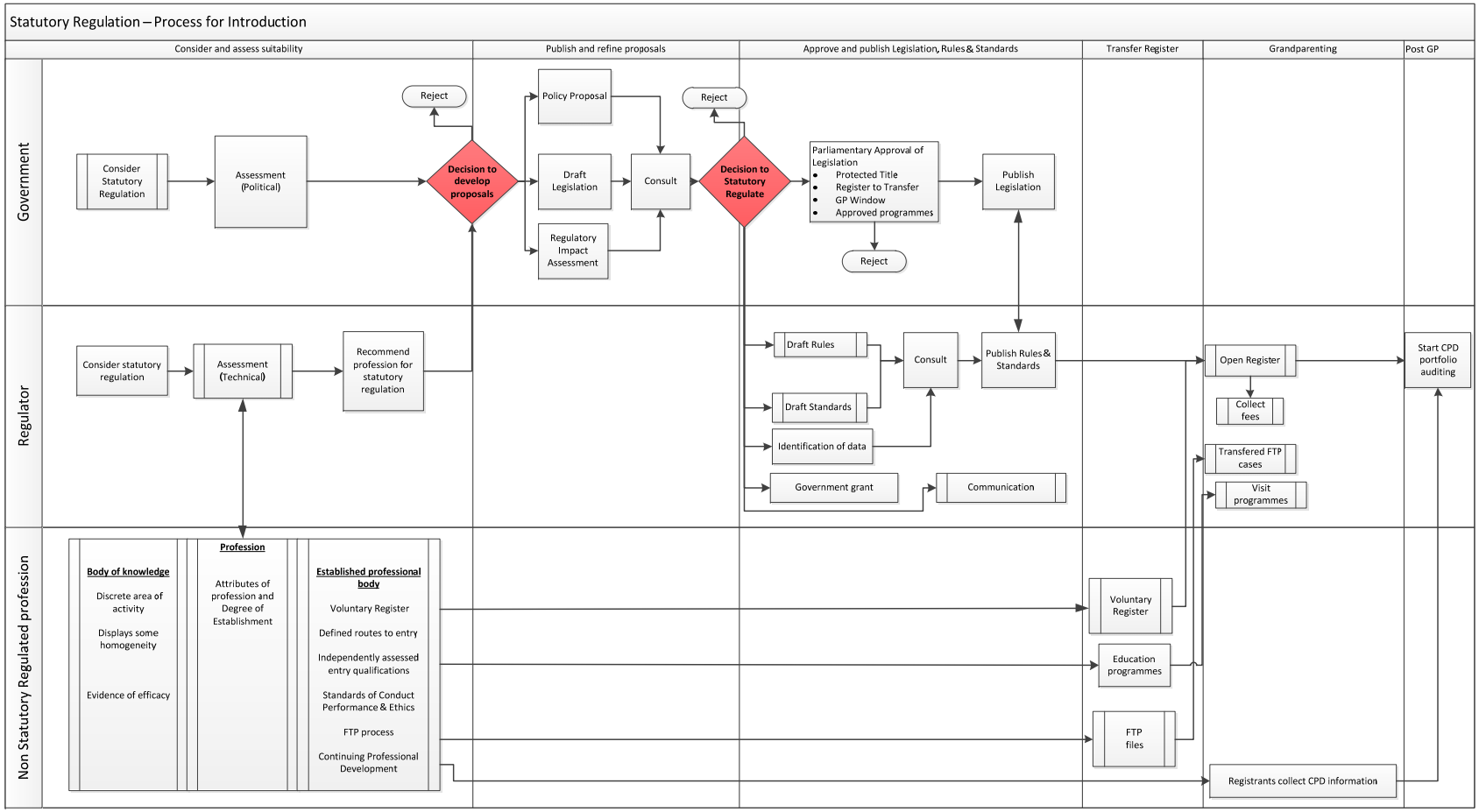
Other ISO standard benefits

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



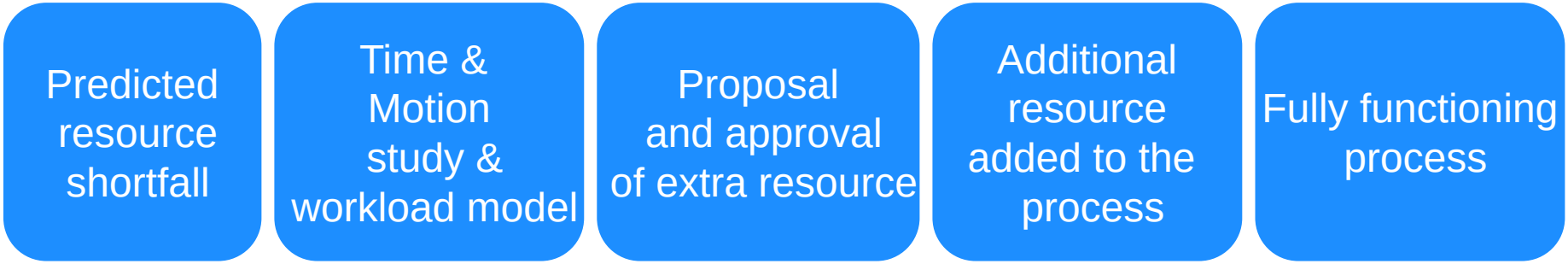
Design it; Run it; Audit it; Fix it. Start again.

Sample process
Statutory Regulation – Process for Introduction



ISO 9001 Standard in action

Worked example – Partner appraisal / assessment process

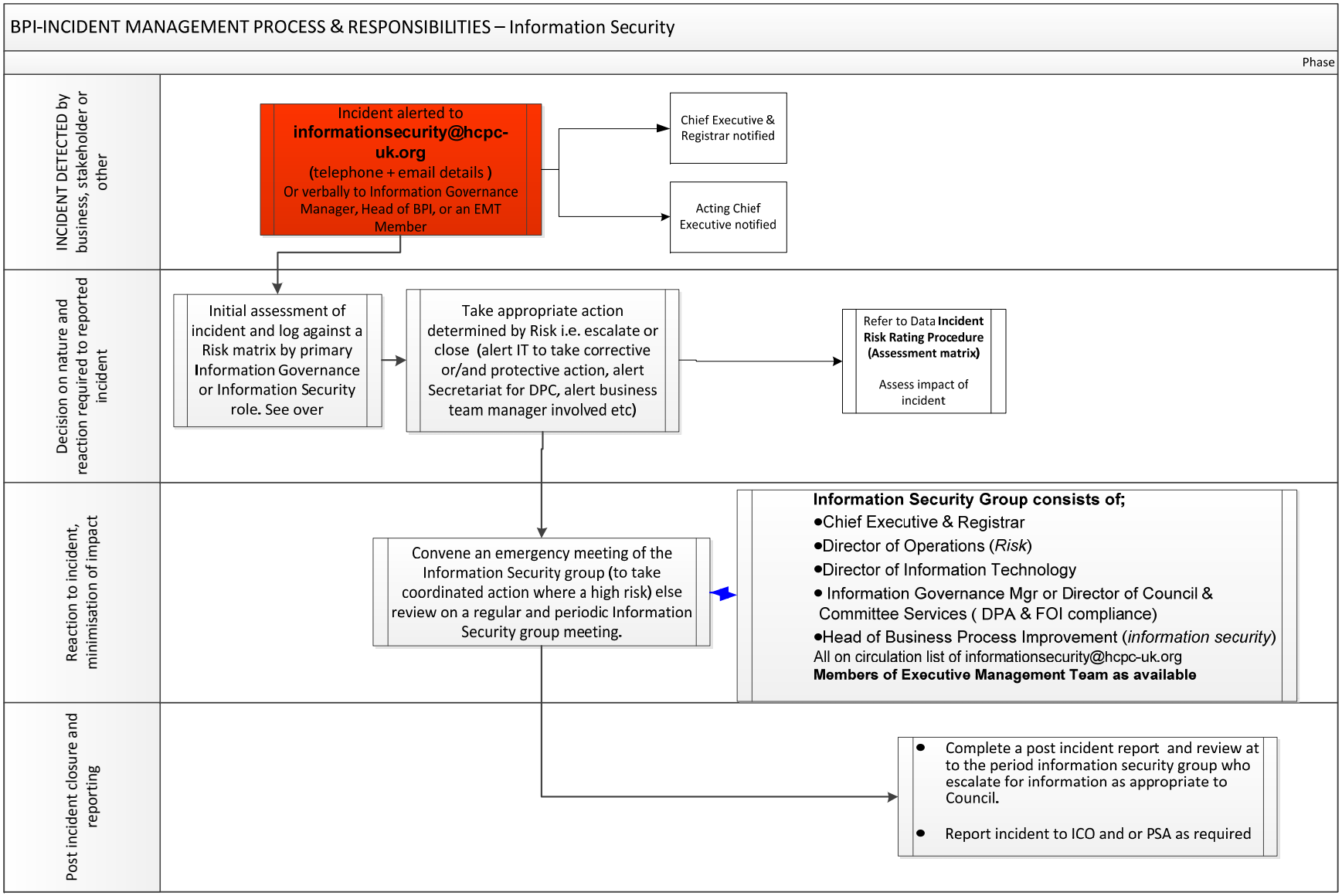


ISO27001:2013 Information Security

- 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

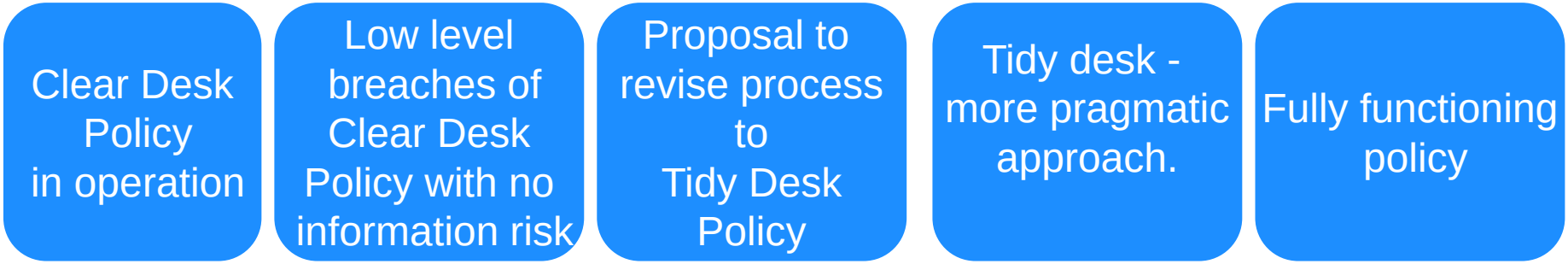
Ite	Asset	Impact - confide ntiali	Impact - integri ty	Impact - availab ility	Risk	Confid entiali ty	Integri ty	Availab ility	Likelih ood - confi ntiali	Likelih ood - integ ty	Likelih ood - avail ility	Risk rating - confi ntiali	Risk rating - integ ty	Risk rating - avail ility	Control	Control refere ce	Reside al risk rating confi	Reside al risk rating integ	Reside al risk rating avail	State
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 service	A.15.2.1	3			OK
77	NetRegulate exported print files		3		Unauthorized 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		Unauthorized actions: Corruption of data due to Personnel: Lack of monitoring mechanism	n/a	Yes	n/a		2			6		Protection of records	A.18.1.3		6		OK

Sample ISO27001 process, part of Incident Management



ISO 27001 Standard in action

Worked example – information stored on desks



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

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

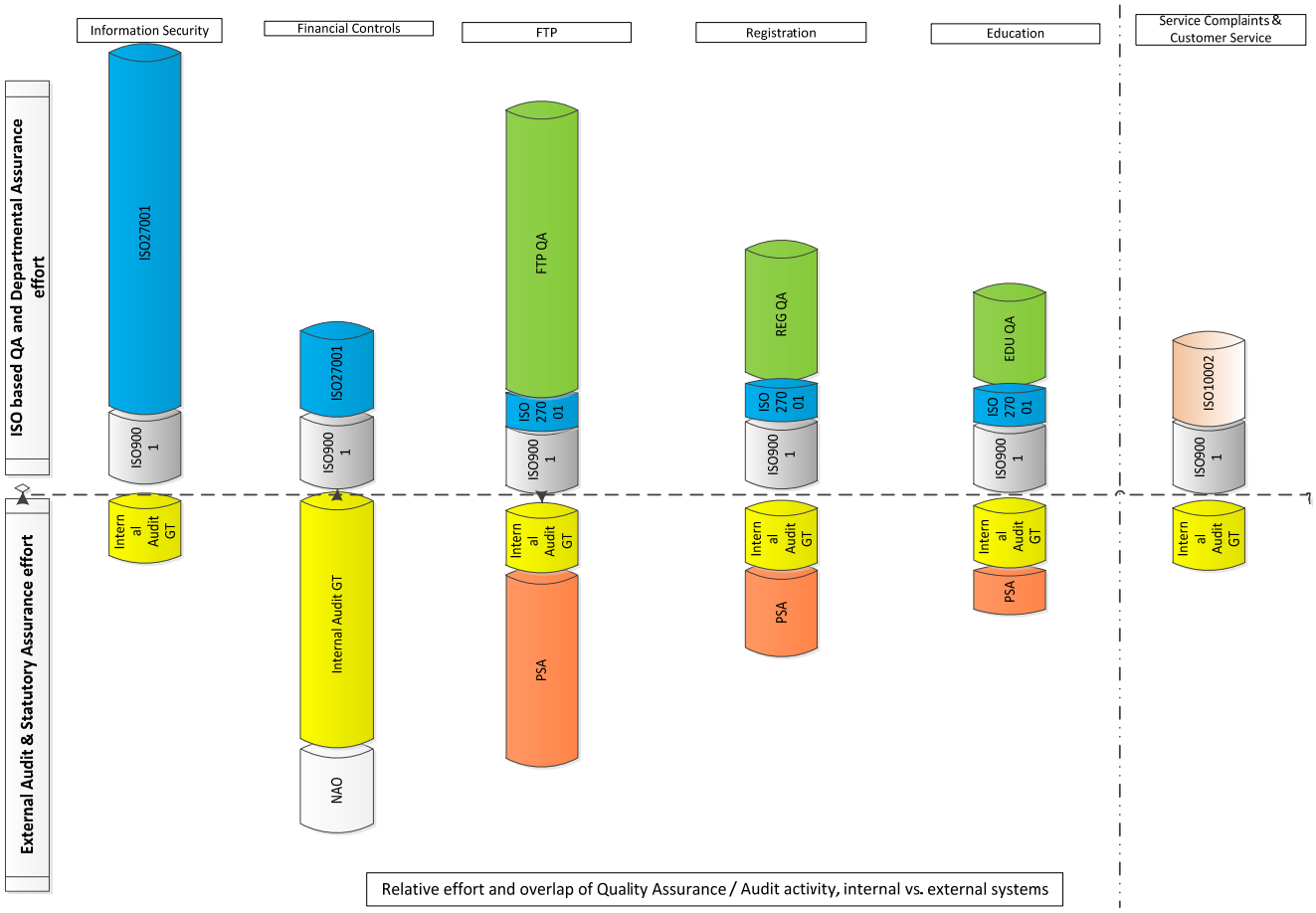
BSI external audits
4 days ISO9001 pa,
2 days ISO27001 pa,
2 days ISO10002 pa

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

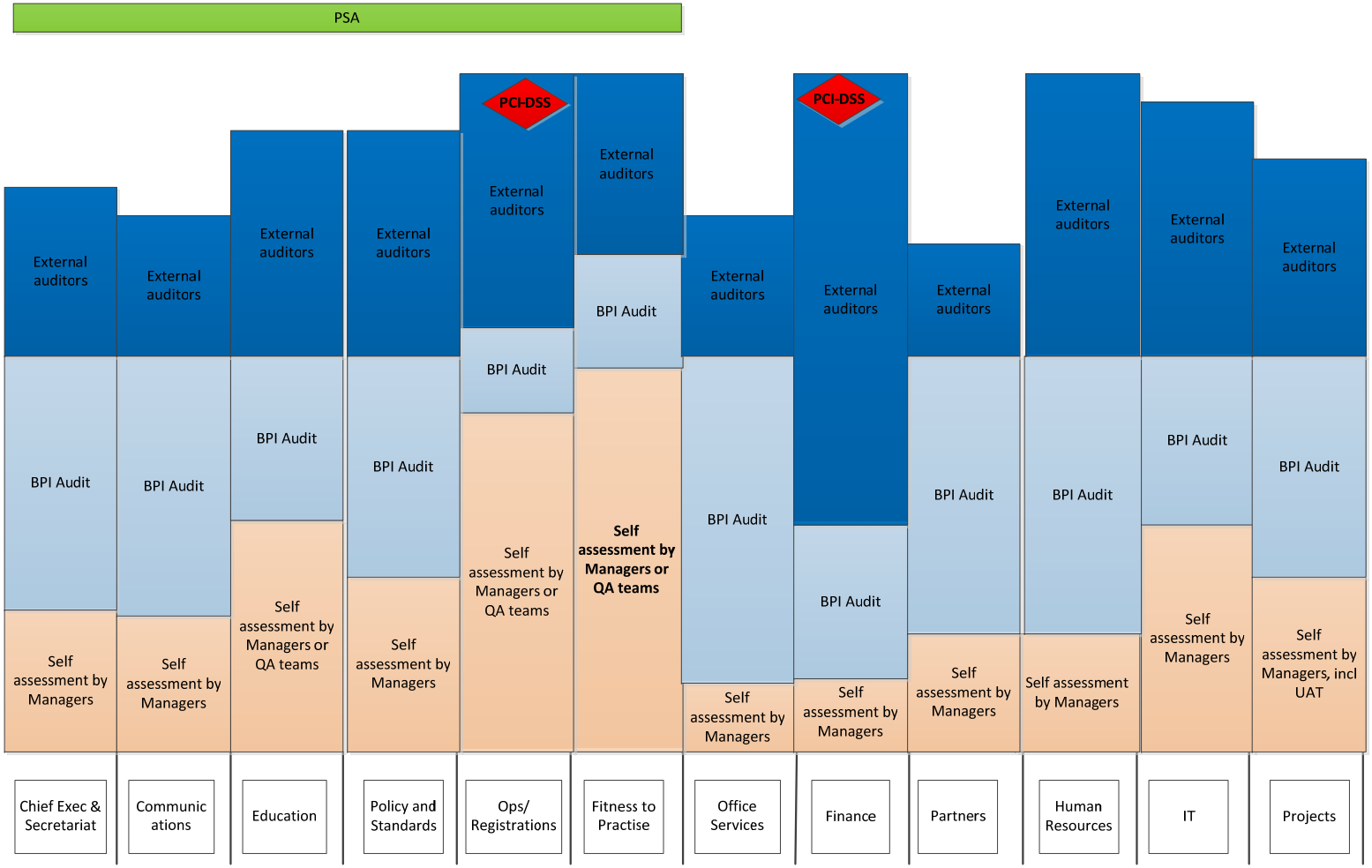


Key

- 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

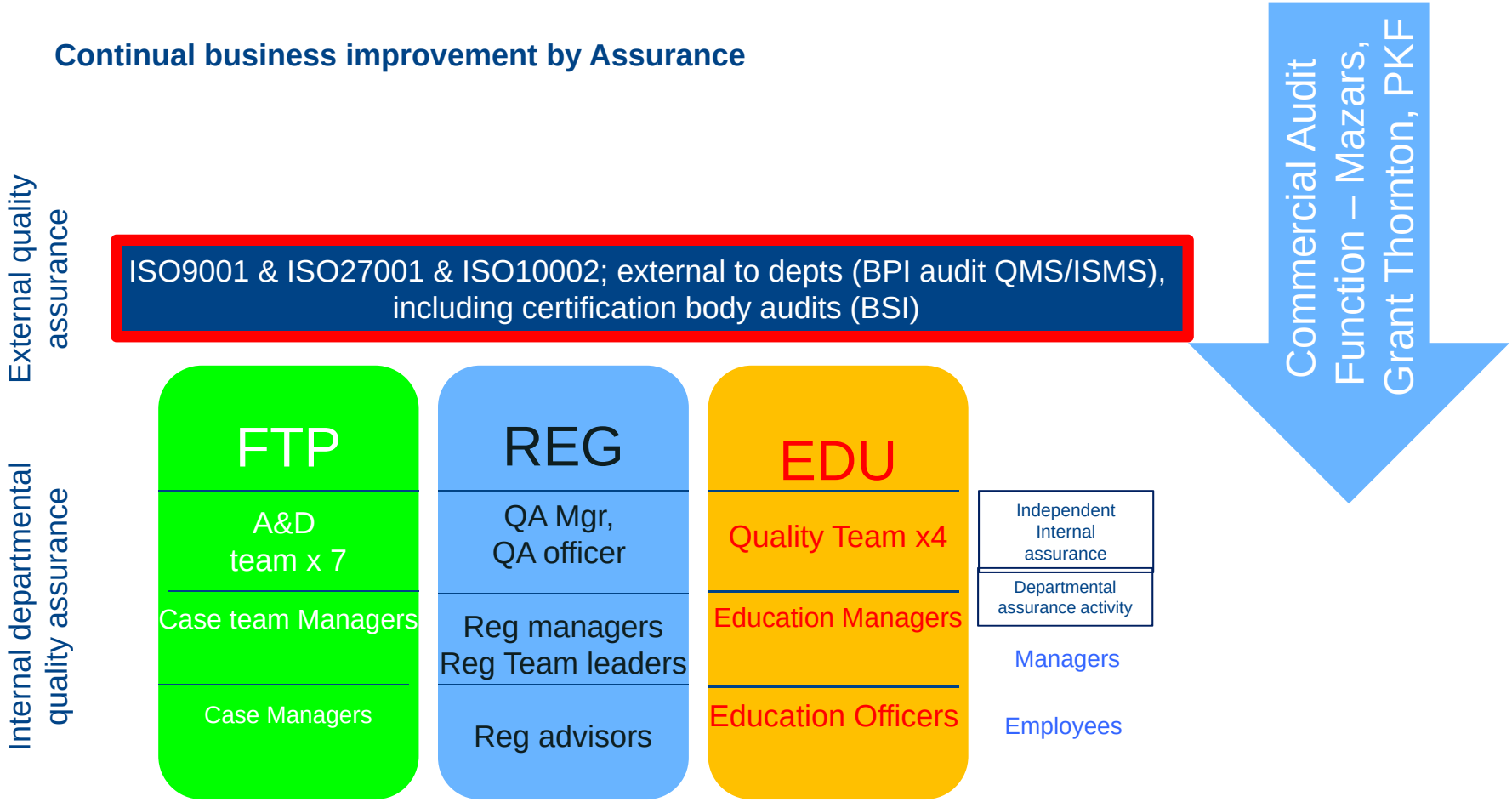
HCPC's audit across all departments

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



HCPC's internal assurance effort by internal department teams

Continual business improvement by Assurance



HCPC's QMS – processes in ISO9001

Information Security
ISO27001:2013

Stakeholders

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

Privy Council

Governance

Council

Plan

Secretariat & Customer Service

Public

Communications

Fitness to Practise

Policy & Standards

Education

Registrations

Registrants (Practitioners)

Users of Registered Practitioners

Public

Act

Executive Management Team

Operations

Support Services

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

Cross Directorate Team

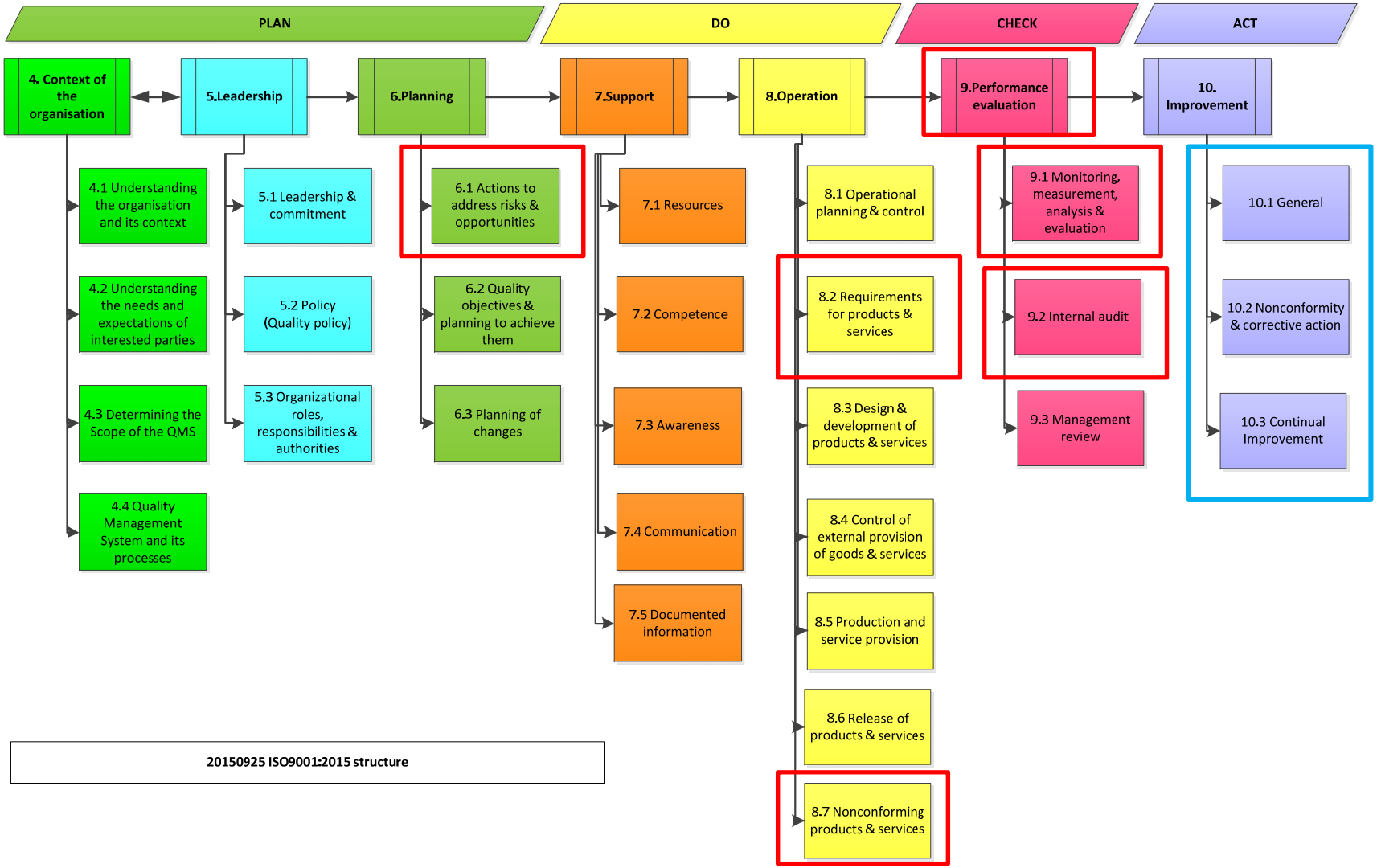
Do

Check

Safeguard Health and Well-being of Users

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

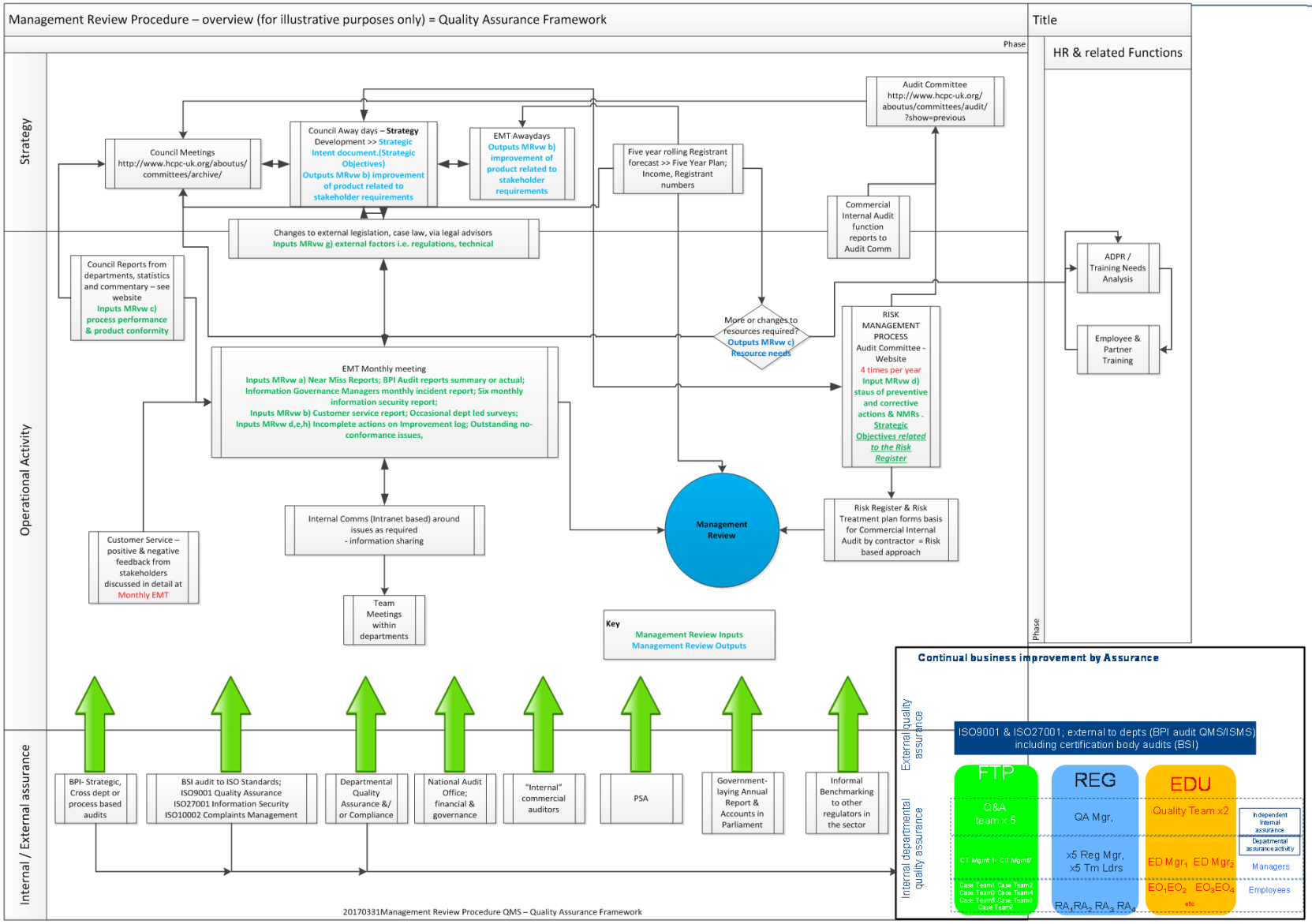
ISO9001:2015 Quality management systems



ISO27001:2013 Information security management systems

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. BPI/QM	Incident Date	Date Logged	Raised By	Type	Description of Finding/Issue BPI/QM/Internal Auditor	Root cause. N/A if no Observation or NC's found in audit BPI/QM/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 = Yello'' 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 BPI/QM/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 occurrred	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?