General Medical Council

Regulating doctors
Ensuring good medical practice

To consider

Report of the Audit and Risk Committee

Issue

1 A summary of the Audit and Risk Committee's activities since it reported to Council on 10 December 2013.

Recommendation

2 Council is asked to consider the report of the Audit and Risk Committee.

Report of the Audit and Risk Committee

Issue

3 The Audit and Risk Committee is required by its Statement of Purpose to report to Council at least twice a year; it last reported to Council on 10 December 2013.

Purpose and membership

4 The Committee is a governance committee of Council. It comprises six Council members and two co-opted external members. The Chair is Hamish Wilson.

5 As set out in its Statement of Purpose, the Committee is responsible for ensuring the integrity of our financial statements; reviewing the systems of internal control, governance and risk management; and monitoring and reviewing both the internal and external audit services.

Meetings

6 Since its last report to Council, the Committee met on 25 February and 29 April 2014.

Trustees' Annual Report and Accounts for the Year Ended 31 December 2013

7 On 29 April 2014, the Committee considered the Annual Report and Financial Statements for the year ended 31 December 2013. Through discussion with the external auditors, the Assistant Director of Finance and Procurement, and the Director of Resources and Quality Assurance, the Committee satisfied itself that the accounts were properly prepared and were in accordance with the Charities Act 1993 and applicable accounting standards.

8 The Committee considered the Management Letter from Crowe Clark Whitehill, which confirmed that the external auditors were satisfied in respect of audit and accounting matters, and that no significant weaknesses in financial systems and controls were identified.

Risk Management

9 As the trustees of a registered charity, Council is required to make a positive statement in the Annual Report, confirming that the major risks to which the charity is exposed, as identified by the trustees, have been reviewed, and that systems have been established to mitigate those risks. The Audit and Risk Committee reviews the risk management arrangements and the Corporate Risk Register periodically to support Council in meeting this requirement. The Committee last reviewed the Corporate Risk Register on 29 April 2014.

Internal audit

10 Internal audit is resourced by an in-house head of the service, and Grant Thornton, an external service provider. The three year contract with Grant Thornton was extended for an additional year and is due to expire on 4 January 2015.

11 In line with best practice, the Committee recently commissioned an external quality assurance and consideration for future directions report on internal audit (IA). The results show that 'the GMC IA Service generally conforms to 49 out of the 56 principles in the International Professional Practice Framework for internal auditing and partially conforms to the remaining seven'. The report said that 'internal audits are carried out objectively, in a systematic and disciplined way, and the assurance offered is independent of undue management influence'. On the basis of the review and the considerations for future direction provided, the Committee has decided that an enhanced co-sourcing model, with additional senior level in-house resources, a contract with an external organisation and clear accountabilities for the work presented to the Committee, would be appropriate.

12 Internal audit delivers an annual programme of reviews in order to provide independent assurance on the adequacy and effectiveness of the systems of risk management, governance, and internal control.

13 On 29 April 2014, and then following an update on circulation on 8 May 2014, the Committee considered the Head of Internal Audit Opinion over the systems of governance, risk management and internal controls in operation during 2013, and noted that Substantial assurance was awarded (based on the agreed assurance model). The opinion is included in the Internal Audit Annual Report at Annex A.

14 Since its last report, the Committee has rigorously scrutinised the outcomes of three scheduled reviews which have been presented by the internal audit service. It has probed in detail and on occasions challenged findings from individual reports, and sought and received assurances from management regarding the actions proposed to address the issues identified.

15 The recent reviews are: Preparations for the outcome of the Home Office review of the Notifiable Occupations Scheme; Fitness to Practise Investigation Reforms - Pilot of Facilitated Meeting with Doctors; and Availability of Business Critical IT systems. Each review was awarded one of the top two GMC internal audit levels of assurance (Sound or Substantial).

16 At each meeting, the Committee received a progress report, including an update on the status of actions arising from internal audit work; on 29 April 2014, as part of the Internal Audit Annual Report, it received a fuller analysis of the actions generated from the 2013 programme of work. The

Committee noted that a significant majority of actions arising from the 2013 programme of work had been implemented by management and looked carefully at the actions that were still outstanding. The Committee requested that the Executive review the schedule of outstanding actions to identify any actions that had been implemented and any that had become redundant, since the completion of the latest follow up exercise. This has now been completed and the current position is reflected in the updated Internal Audit Annual Report at Annex A.

2014 programme of internal audit work

17 On 6 November 2013, the Committee approved an interim programme of internal audit work for the first part of 2014 pending the outcome of the fundamental review of risk management and the development of the Corporate Strategy, Business Plan and associated risk registers. On 29 April 2014 the Committee considered and approved a schedule of audit areas for the rest of 2014.

18 The full programme of work for 2014 is presented at Annex B. Ten of the 11 reviews in the plan, including the ones previously agreed in the interim programme of work, are aligned to risks in the current Corporate Risk Register. The Committee requested a review in relation to fraud control measures, an area that is not explicitly reflected in the Corporate Risk Register.

Significant Event Reviews

19 Since the Committee last reported to Council, it has noted the outcomes of nine Significant Event Reviews and the actions taken or proposed by management.

Supporting information

How this issue relates to the corporate strategy and business plan

27 The Audit and Risk Committee is responsible for ensuring the integrity of our financial statements; reviewing our systems of internal control, governance and risk management; and for monitoring and reviewing both the internal and external audit services. As such, it plays a vital role in our governance framework and relates to all areas of our Corporate Strategy and Business Plan.

If you have any questions about this paper please contact: Ellen Wright, Head of Consultancy and Review Service, ewright@gmc-uk.org, 0207 189 5023.

General Medical Council

Regulating doctors
Ensuring good medical practice

Annex A

Internal Audit Annual Report

1 The annual internal audit report for the year ended 31 December 2013, and the Head of Internal Audit Opinion on the systems of governance, risk management and internal control in operation throughout the year, was considered by the Audit and Risk Committee at its meeting on 29 April 2014.

2 At that meeting the Committee asked that that several revisions be made to the report. The revised report was circulated to the Committee for comment and agreement on 8 May 2014.

On circulation – 8 May 2014

Audit and Risk Committee

General Medical Council

Regulating doctors
Ensuring good medical practice

To consider

Internal Audit Annual Report

Issue

1 The annual internal audit report for the year ended 31 December 2013, and the Head of Internal Audit Opinion on the systems of governance, risk management and internal control in operation throughout the year.

Recommendations

2 The Audit and Risk Committee is asked to consider:

a The adequacy of the internal audit work conducted during 2013.

b The Head of Internal Audit Opinion on the systems of governance, risk management and internal control operating in 2013.

Internal Audit Annual Report

Issue

Internal audit's role and positioning within the governance framework

3 Our internal audit service is referred to as the Consultancy and Review Service (CRS). It is resourced using a co-sourcing model comprising of an in-house head of internal audit (the Head of Consultancy and Review Service) and audit personnel from Grant Thornton, an external accountancy, audit and advisory firm. The function conducts a range of activities aimed at providing independent assurance to senior management and to Council, through the Audit and Risk Committee, in respect of governance, risk management and internal control. Through its programmed, responsive and ad hoc work, CRS also provides challenge and support to managers across the organisation, facilitating on-going improvement in the control environment.

4 The purpose of the *Head of Internal Audit Opinion* is to contribute to the assurances available to the Audit and Risk Committee and to Council which underpin their own assessment of the effectiveness of the systems of governance, risk management and internal control. The *Head of Internal Audit Opinion* assists the Committee and Council in approving the assurance statements included in the published Annual Report and Accounts.

5 The Audit and Risk Committee approves an annual programme of internal audit reviews, the outcomes of which contribute to the annual *Head of Internal Audit Opinion*. Insights from other work, such as Significant Event Reviews, also contribute to the Opinion.

Head of Internal Audit Opinion

6 Overall opinion:

> Substantial assurance can be given that the systems of governance, risk management and internal control in operation during 2013 were generally well designed and working effectively to ensure the achievement of the GMC's objectives. Some significant areas for improvement were identified during the year and they have either been addressed or are scheduled to be addressed.

Basis for opinion

7 The opinion is based mainly on the following:

a Insight to fundamental aspects of the control environment during 2013.

b Outcomes of the 2013 risk-based internal audit reviews.

c Significant Event Reviews undertaken during the year.

Commentary

Assurance level

8 In accordance with the established framework, the *Head of Internal Audit Opinion* is given in the context of the four levels of assurance that are used in the grading of the individual audit reports as these are outlined in the table at Appendix B.

Control environment

9 In arriving at the Opinion, consideration was given to fundamental aspects of the control environment, including arrangements for:

a Establishing and monitoring the achievement of the organisation's objectives.

b Decision-making.

c Financial management and reporting.

Internal audit activities conducted during 2013

10 A summary of 2013 internal audit activities is below:

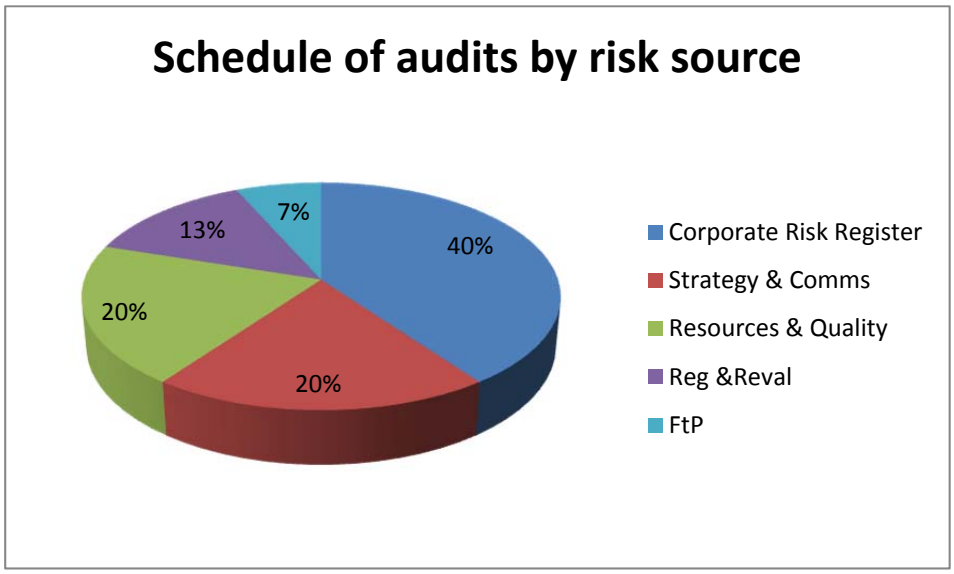
Nature of Activity	Work Undertaken in 2013
Programmed reviews	14 scheduled reviews and three spot checks completed and reported to the Committee. The review of Governance was rescheduled to 2014 with the Committee's approval. The remaining review, Business Planning, Risk Management and Performance monitoring is at draft report stage. Transaction cost of delivering the 2013 programme of work is expected to be slightly under budget, at £137,000, provided the outstanding review is delivered in line with the estimated cost.
Significant Event Reviews (SERs)	Guidance, challenge, coordination and reporting in respect of 10 SERs completed during the year and a further seven in progress at the year end and carried forward to 2014.
Follow-up on agreed actions	Follow up on actions arising from internal audit work to ensure they are implemented, and reporting of progress to the Committee.

Programmed Reviews

11 The programme of reviews for 2013 was approved by the Audit and Risk Committee on 21 November 2012. It was considered by the re-constituted Committee at its first meeting on 30 April 2013 and has been reviewed at each meeting during the year.

Analysis of programmed reviews conducted in 2013

12 The programme of reviews was developed on a risk basis, the audit topics reflecting critical or significant risk areas drawn mainly from the Corporate Risk Register. Some risk areas were drawn from directorate risk registers as they were considered to be significant, although not reflected in the Corporate Risk Register. The graph below analyses the 2013 programme of reviews by risk source. The schedule of audits is at Appendix B.



Overview of issues identified through 2013 programmed reviews

13 Audit reviews assess the extent to which effective internal controls have been established to manage specific risks, and the degree of compliance with those controls. The large majority of issues identified through our reviews in 2013 did not arise from any fundamental flaws in the control design or any systematic non-compliance. Rather, the issues were identified to facilitate improvement to the controls.

14 Common themes emerging from a 2013 audits include:

a Three highlighted that there were limitations in the systems that were preventing the analysis or filtering of data held. Conversely, two further audits identified that manual processes were being applied instead of the automated ones available.

b Four audits identified a lack of procedure notes governing when certain processes or workflows should be followed.

c The need to carry out and report on post-implementation/benefit realisation reviews was identified in three audits.

d Two reviews identified that the auditors were not able to see evidence supporting management's assertions that certain controls and checks had been carried out.

Actions arising from 2013 reviews

15 The programme of work for 2013 gave rise to 46 agreed actions; there were no unresolved issues giving rise to any rejected recommendations. Three of the actions were ranked as High Priority, in accordance with the definitions set out at Appendix A. The three High Priority actions arose from the review of Education Quality Assurance - Post visit monitoring and the use of Checks (Short targeted visits). They were all implemented by 7 May 2014. The three High Priority actions are set out below:

a Ahead of the Quality Team's next review of actions taken by Local Education and Training Boards and Deaneries, establish clear guidelines for the review and documentation process. Staff guidance to set out how evidence should be reviewed prior to actions being closed, how staff should record their analysis of the evidence to support their decision to close an action, specify the need to build in review timescales in order to discuss any proposed decisions to close actions.

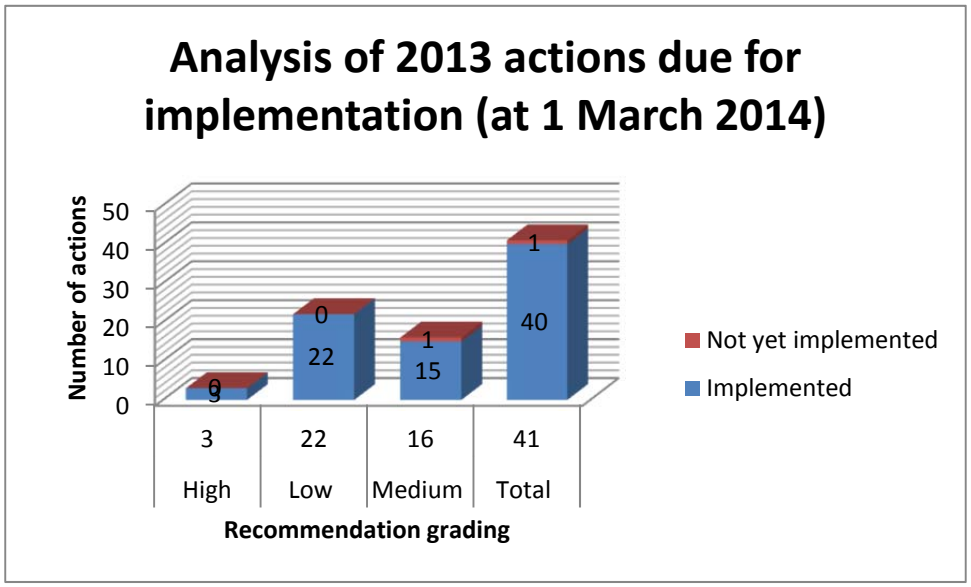
b As the review and assessment of actions is a new process to many people completing it, introduce additional oversight. The Head of Quality, when reviewing the feedback letters produced at the end of the scrutiny process, should sample check the decisions, referring back to the visit and monitoring teams any that they consider to be a wrong decision, or any that is not supported by sufficient analysis of the evidence.

c Consider whether the current approach to reviewing recommendations remains appropriate, given existing resource levels. Should time pressures continue, a decision should be taken to either increase resources or reduce the level of scrutiny over low-risk actions.

Follow up

16 At each meeting throughout 2013, the Committee received a status report in respect of the 2013 actions and outstanding actions from previous years.

17 The 2013 programme of work generated 46 actions (excluding any actions from the business planning, Risk Management and Performance Management report which is still in draft). 41 of these actions were due to be implemented by 1 March 2014. By 7 May 2014, 40 of those actions were implemented, as well as one which was not yet due for implementation. The one remaining overdue action, together with three actions (one ranked as medium priority) from the 2012 programme of work are expected to be implemented by December 2014. The graph below analyses the 41 agreed actions from the 2013 programme of work that have fallen due for implementation, by priority and status.



Significant Event Reviews (SERs)

18 A significant event is defined as an incident that has the potential for a material adverse effect on the organisation. When such events occur unexpectedly, a Significant Event Review is conducted to investigate how the incident occurred, to strengthen any control weaknesses, and to share learning. The head of the internal audit function is responsible for providing written and informal guidance for the conduct of SERs; providing support and challenge to ensure the robustness of the investigations; and for coordinating and reporting on the progress and outcomes of SERs. During 2013, 10 SERs were completed, the outcomes of which have been reported to the Committee. A further seven SERs that commenced in 2013 were still in progress at the end of the year and were carried over to 2014.

Supporting information

How this issue relates to the corporate strategy and business plan

11 The programme of internal audit work provides independent assurance. It contributes substantially to the overall assurance that the systems of internal control and risk management are adequate and are operating effectively to support the achievement of our corporate aims and objectives. Progress reports enable the Committee to satisfy itself regarding the extent to which audit work is delivered in the expected timeframe; to explore any issues affecting the delivery of the programme of work; and to assess the extent to which management is taking actions to address the issue identified through the internal audit work.

Other relevant background information

12 The Head of Consultancy and Review Service was supported by Grant Thornton in the delivery of the 2013 programme of internal audit work.

What equality and diversity considerations relate to this issue

13 Equality and diversity issues are considered in the planning and delivery of the programme of audit work.

If you have any questions about this paper please contact: Ellen Wright, Head of Consultancy and Review Service, ewright@gmc-uk.org, 020 7189 5023.

General Medical Council

Regulating doctors
Ensuring good medical practice

Appendix A

Assurance rating and priority ranking

Assurance Definitions

Assurance Level	Definition
Sound	Controls evaluated are sufficient, and appropriate, and are operating effectively to provide assurance that risks are being managed and objectives should be met.
Substantial	A few specific weaknesses were noted. Generally, however, controls evaluated are sufficient and appropriate, and are operating effectively to provide assurance that risks are being managed and objectives should be met.
Limited	Many specific control weaknesses were noted. Controls evaluated are unlikely to provide assurance that risks are being managed and objectives should be met.
Minimal	Controls evaluated are not adequate, appropriate or effective to provide assurance that risks are being managed and objectives should be met.

Priority ratings

Priority Level	Definition
High	The issues identified pose substantial risks to the organisation. For the attention of the Audit and Risk Committee.
Medium	The issues identified are of moderate risk to the organisation.
Low	The issues identified are of low risk to the organisation, but the benefits of addressing them outweigh the cost.

General Medical Council

Regulating doctors
Ensuring good medical practice

Appendix B

2013 Programmed Reviews

1 The schedule below sets out the programme of reviews for 2013, together with an indication of when the outcomes were reported to the Audit and the assurance levels awarded.

	Project Title Per 2013 Audit Plan	Timetable				Status	Comment	Assurance Level
		Q 1	Q 2	Q 3	Q 4			
1	New governance arrangements (with a detailed focus on Education Governance Structures)					Deferred to 2014	Agreed by the Committee on 30 April 2013	
2	Business planning, risk management and performance reporting					Draft report stage		
3	Communication with doctors					Completed	Reported on 25 June 2013	Substantial
4	Enhancing engagement					Completed	Reported on 6 Nov 2013	Sound
5	Transfer of Activities to Manchester - Benefits Realisation					Completed	Reported on 5 Sep 2013	Sound
6	Core Financial Controls: Payroll					Completed	Reported on 30 April 2013	Substantial
7	Availability of Business Critical IT systems					Draft report stage		
8	*ISO 27001and BS 10008 Compliance					Completed	Reported on 5 Sep 2013	Substantial
9	International Medical Graduate Route to Registration					Completed	Reported on 30 April 2013	Sound
10	Integrity of Registration Performance Information					Completed	Reported on 25 June 2013	Substantial

	Project Title Per 2013 Audit Plan	Timetable				Status	Comment	Assurance Level
		Q 1	Q 2	Q 3	Q 4			
11	Registration projects					Completed	Reported on 25 June 2013	Substantial
12	Revalidation - post launch review					Phase 1 completed Phase 2 deferred	Reported on 5 Sep 2013	Sound
13	Preparations for the outcome of the Home Office review of the Notifiable Occupations					Completed	Report on agenda	Sound
14	Fitness to Practise Investigation Reforms - Pilot of Facilitated Meeting with					Completed	Report on agenda	Sound
15	Medical Practitioners Tribunal Service - post launch review					Completed	Reported on 5 Sep 2013	Substantial
16	Operation of quality assurance arrangements for medical education					Completed - scope revised	Reported on 6 Nov 2013	Substantial
17	Spot Check 1 – Fee Income					Completed	Reported on 30 April 2013	N/A
18	Spot Check 2 – MPTS** Selection of Panellists – Equality & Diversity Considerations					Completed	Reported on 25 June 2013	N/A
19	Spot Check 3 – Cheque Authorisation					Completed	Reported on 5 Sep 2013	N/A

** ISO 27001 is an International information security standard and BS 10008:2008 is the British standard relating to the legal admissibility and evidential weight of electronic information.*

***MPTS: Medical Practitioners Tribunal Service*

General Medical Council

Regulating doctors
Ensuring good medical practice

Annex B

2014 Programme of internal audit work

		Internal Audit Topics identified from Corporate Risk Register - 10 March 2014							
		Note: the schedule below incorporates the six topics already included in the approved 2014 interim programme of work , as indicated in columns A and C.							
		Five additional eviews and three spot checks have been agreed for 2014.							
		The proposed audit topics are in bold in Column C and the scopes are in Column I.							
Proposed audit year	**Ref**	**Proposed Audit Topic**	**Strategic Aim**	**Deliverable**	**Risk Ranking (before mitigation) and Dscription**			**Scope of Audit Review**	**Est. Audit Days**	**Senior Management Comment**
New	1	**Preparations for possibility of a single legislative framework for healthcare professional regulation.**	***Strategic and Political***	*Ensuring the GMC responds to change resulting from the Law Commission consultation and the resulting Government Bill.*		***CRR 2*** *- The Law Commissions' DH(E) on a single simplified legislative framework for healthcare professional regulation poses a risk to our regulatory independence.* *- Other political priorities cause Govt not to proceed with a Bill. -The Government and PSA may force through a degree of harmonisation that is contrary to our policy intentions/public interest. This is less tangible and more long term.* *- The risk also presents a potential opportunity for us to strengthen our regulatory powers.*		Quality of engagment with the Law Commission and Department of Health (England), monitoring of its impact, and preparations for the implications of a new legislative framework.	18	Subject to the Legislation proceeding or the bill for pre-legislative scrutiny
New	2	**Operational Readiness for English Language Testing**	***Strategic Aim 1:*** *Make the best use of intelligence about doctors and the healthcare environment to ensure good standards and identify risks to*	*Ensuring an appropriate registration framework is in place.*		***CRR 5*** *- We are unable to test the English language proficiency of EEA doctors and consequently we may grant a licence to a doctor from the EEA who is not sufficiently proficient in English to practise safely.*		Extent to whch operational processes for delivery of English language testing have been developed, and are adequate in peparation for the granting of legislative powers.	15	
Approved 2014 Interim Plan	3	**Medical Education - Quality Assurance Arrangements** **(***2014 Interim Plan Q2)*	***Strategic Aim 2:*** *Help raise standards in medical education and practice*	*Demonstrate by 2013, significant progress towards a coherent and proportionate system for regulating all stages of medical education and*		***CRR 12*** *- Significant external factors including the establishment of Health Education England, the creation of new Local Education and Training Boards (LETBs) and the outcomes of the Review of the Shape of Postgraduate Education and Training may impact on our ability to carry out our regulatory functions.*		Extent to which the outcomes of the quality assurance consultation are reflected in implementing feasible and fit for purpose quality assurance arrangements	8	
New	4	**Postgraduate Medical Examinations**	***Strategic Aim 2:*** *Help raise standards in medical education and practice*	*Approval of curricula for specialties and sub specialties.*		***CRR 15*** *- Failure to adequately handle and address concerns about the fairness of Royal College of General Practitioners (RCGP) CSA exams could lead to a loss of confidence in the exam process and reputational damage for the GMC.*		Arrangements for understanding and addressing issues of fairness in Postgraduate Medical Examinations	25	Q4 - in view of ongoing legal action
New	5	**Management of increased volumes of fitness to practise cases**	***Strategic Aim 3:*** *Improve the level of engagement and efficiency in the handling of complaints and concerns about patient safety*	*Ensure we take appropriate and timely action when a doctor's fitness to practise is questioned*		***CRR 16*** *- • A sustained rise in the number of new Stream 1 cases in 2013 (a 9% increase year on year) may result in slower processing times and an increased error rate.* *• Slower processing times could lead to a failure to meet our published service targets/a rise in the average length of cases (a measure of performance that is published by PSA annually).* *• The increased workload could also lead to an increase in processing errors as work volumes per member of staff increase.*		Arrangements for forecasting, and planning for volume changes and for dealing with the impact of increased volumes on service targets and staff workloads.	15	

Internal Audit Topics identified from Corporate Risk Register - 10 March 2014

Note: the schedule below incorporates the six topics already included in the approved 2014 interim programme of work , as indicated in columns A and C.

Five additional eviews and three spot checks have been agreed for 2014.

The proposed audit topics are in bold in Column C and the scopes are in Column I.

Proposed audit year	Ref	Proposed Audit Topic	Strategic Aim	Deliverable	Risk Ranking (before mitigation) and Dscription	Scope of Audit Review	Est. Audit Days	Senior Management Comment
Approved 2014 Interim Plan	6	**Integrity of Fitness to Practise Performance Information** *(2014 Interim Plan Q1)*	***Strategic Aim 3:*** *Improve the level of engagement and efficiency in the handling of complaints and concerns about patient safety*	*Ensure we take appropriate and timely action when a doctor's fitness to practise is questioned*	***CRR 16*** *- • A sustained rise in the number of new Stream 1 cases in 2013 (a 9% increase year on year) may result in slower processing times and an increased error rate.* • *Slower processing times could lead to a failure to meet our published service targets/a rise in the average length of cases (a measure of performance that is published by PSA annually).* • *The increased workload could also lead to an increase in processing errors as work volumes per member of staff increase.*	Through significant levels of testing checking the accuracy of Fitness to Practice performance information reported to senior management, Council and its committees, and external organisations. Checking the validity of the underlying data, the integrity of automated algorithms, and any manual manipulation of	8	
Approved 2014 Interim Plan	7	**Core financial system – Purchasing and Payment (***2014 Interim Plan Q1 - in progress)*	***Strategic Aim 5:*** *Work better together to improve our overall effectiveness, our responsiveness and the delivery of our regulatory functions*	*Ensuring economy, efficiency, and effectiveness in budgetary planning and financial control and to continue to deliver annualised improvements in the unit costs of our operations of between 3% and 5%.*	***CRR 22*** *- • Expenditure or income falls materially outside the budget.* • *Failure to properly cost projects and activities.* • *Failure to adhere to agreed financial controls or schedule of delegations.* • *Difficulty in identifying savings whilst maintaining high quality of business-as-usual and ambitious work programmes.* • *Failure to operate procedures to minimise the risk of fraud.*	The effectiveness and efficiency of, and compliance with, purchasing and payment controls. The review will cover purchase ledger transactions, including those relating to agency staff.	10	
New	8	**Fraud Prevention and Detection Measures** (Audit and Risk Committee's request)	***Strategic Aim 5:*** *Work better together to improve our overall effectiveness, our responsiveness and the delivery of our regulatory functions*	Ensure that appropriate control measures to prevent and detect fraud are in place. (This Deliverable is not reflected in the CRR, but arose from a discussuiion at the ARC meeting on 29 April)	The CRR does not reflect a specific risk relating to this audit area; the issue arose from a discussion at the ARC meeting on 29 April.	Review of the corporate approach to fraud prevention and detection. Evaluation of the extent to which control measures have been built into operational and financial processes to prevent and detect different types of fraud (such as diversion, backhander and inducement), and the extent to which those controls have been reviewed.	18	
Approved 2014 Interim Plan	9	**Compliance with ISO 27001 and BS 10008** *(2014 Interim Plan Q2)*	***Strategic Aim 5:*** *Work better together to improve our overall effectiveness, our responsiveness and the delivery of our regulatory functions*	*Ensure that we remain vigilant in the face of information security threats.*	***CRR 26*** *- • Inadvertent or malicious disclosure of information.* • *Malicious attempts to access or compromise our IT network.* • *Malicious attempts to access our offices*	Annual reviews against the information security standard, ISO 27001, and BS10008, the standard for the legal admissibility of electronic documents. *(Consider whether to include the Payment Card Industry information security standard, PCI in the future)*	12	

Internal Audit Topics identified from Corporate Risk Register - 10 March 2014

Note: the schedule below incorporates the six topics already included in the approved 2014 interim programme of work , as indicated in columns A and C.

Five additional eviews and three spot checks have been agreed for 2014.

The proposed audit topics are in bold in Column C and the scopes are in Column I.

Proposed audit year	Ref	Proposed Audit Topic	Strategic Aim	Deliverable	Risk Ranking (before mitigation) and Dscription	Scope of Audit Review	Est. Audit Days	Senior Management Comment
Approved 2014 Interim Plan	10	**Cyber security penetration testing** *(2014 Interim Plan Q1 - in progress)*	***Strategic Aim 5:*** *Work better together to improve our overall effectiveness, our responsiveness and the delivery of our regulatory functions*	*Ensure that we remain vigilant in the face of information security threats.*	***CRR 26*** *- • Inadvertent or malicious disclosure of information.* *• Malicious attempts to access or compromise our IT network.* *• Malicious attempts to access our offices*	Penetration testing to evaluate the security of a selection of key information systems and networks against cyber attack	18	
Approved 2014 Interim Plan	11	**New Governance Arrangements** *(2014 Interim Plan Q1 - in progress)*	***Strategic Aim 5:*** *Work better together to improve our overall effectiveness, our responsiveness and the delivery of our regulatory functions*	*Ensuring that appropriate structures and processes are in place to enable Council to uphold its responsibilities as the governing body of the GMC.*	***CRR 27*** *- • The role of the reconstituted Council with a reduced size has meant changes to the overall governance framework.* *• The new arrangements may not be effective because:* *- the agreed framework and ways of working are not effectively managed and implemented.* *- there is insufficient clarity and understanding about roles, decision making arrangements and agreed delegations to ensure that the arrangements are effective and support good governance.*	Key aspects of the arrangements for ensuring that the Council is appropriately positioned and is supported in order to ensure that it operates effectively and efficiently; and particularly that it has a clear understanding of how statutory responsibilities are being delivered. The review covers induction; governance structures, roles and responsibilities; and operations, particularly the quality of information presented to Council and the implementation of action arising from Council decisions.	25	
New	12	**Spot Checks x 3:** areas to be identified	*Management Request*				5	
						Total Days	**177**	