General Medical Council

Agenda item:	**M9**
Report title:	**Report of the Audit and Risk Committee**
Report by:	**Lindsey Mallors,** Assistant Director - Audit and Risk Assurance, lindsey.mallors@gmc-uk.org, 020 7189 5188
Considered by:	**Audit and Risk Committee**
Action:	**To consider**

Executive summary

This report provides an update to Council on the Audit and Risk Committee's activities since May 2017. It notes:

- The assurance the Committee continues to receive in the operation of the Risk Management Framework
- There is a good control framework in place across the organisation and internal audit recommendations have appropriate actions in place to address them
- Continued satisfaction with the work of external and internal auditors.

Recommendation

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

Introduction

1 The Audit and Risk Committee has met three times since its last report to Council, in formal session and seminar on 12 July, 14 September (in Manchester) and on 16 November 2017. The seminar in July focused on identifying risks to the GMC emerging from Council's away day discussion and the potential areas for audit assurance in 2018. In September the Committee considered risks associated with the GMC's role in medical education and the work of the Education and Standards Directorate and in November, the work of the IT operations, Information Security, Enterprise Systems and Development and IS Projects and Training teams.

2 Committee meetings continue to be supported by the Executive Team and have included the attendance of relevant directors and assistant directors when audit reports relating to their area of business have been presented. The Committee appreciates the commitment given to meetings which contributes to its assurance on the effectiveness of operational processes, the ongoing ability of management teams and their leadership to follow up and deal with issues arising from audit review and the quality of audit work undertaken.

3 At is meeting on 16 November 2017 the Committee undertook its annual review of its Statement of Purpose and considers this remains relevant for its assurance role with the addition of specific reference to general data protection and cyber security. Both of these reflect risks which are affecting organisations globally and are included in the Committee's internal audit programme on an annual basis.

4 Areas to bring to Council's attention arising from the Committee's responsibilities and activities are outlined below.

Integrity of the financial statements and performance of the external auditor

5 In June, following the work of the external auditors, Crowe Clark Whitehill, Council approved the financial statements and Annual Report 2016. Since then, the Committee has undertaken its annual assessment of the external auditor's performance and continues to hold a positive view of their work and relationship with the Committee. The external audit fee, terms of engagement, external audit plan and audit scope for 2017 were discussed in preparation for the 2017 external audit at the November Committee meeting.

6 The Committee has also met privately with the external auditor since the last report to Council providing an opportunity to discuss any issues without the presence of senior management.

Governance and risk management

7 The Committee continues to use risk as the basis for focus on its approach to oversight and scrutiny. At each meeting it has received a strategic risk update from the Chief Executive, discussed risk with the Chief Operating Officer (COO), and scrutinised the Corporate Risk Register and Corporate Issues Log. These updates and the following discussions are a key focus of meetings ensuring the Committee retains a balanced consideration of forward looking risks and issues alongside its backward look at audit work to gain its assurance on systems of internal control and risk management.

8 This year's internal audit review of risk focused on the management of risk in projects. To maintain independence from the responsibilities for risk which sit with the Assistant Director of Audit and Risk Assurance, the scope for this review was agreed by the Chair of the Committee and the report sent directly to him. The report concluded that risk management within projects is effective and generally in line with good practice. As risk arrangements continue to mature there will be further focus on:

a The interaction between project risk processes and the overall risk management framework, including further understanding of risk interdependencies across our work streams.

b Providing more robust challenge of project risks at all levels of management review.

c Extending the range and number of risks captured on the central reporting platform (Planview) to ensure that there is visibility of a broad range of project risk beyond the corporate project risks which are currently captured.

Systems of internal control

9 A comprehensive risk-based audit programme has been delivered during 2017 with a few changes agreed with the Committee during the year to reflect emerging risks and changes in the wider organisational and external environment. This demonstrates the flexibility of the Committee and audit team in meeting new priority assurance needs.

10 As in previous years, the audit programme has comprised operational compliance based audits, the use of spot checks for short targeted reviews, and audit work on areas with a clear key strategic impact – for example the Medical Licensing Assessment (MLA) and digital media strategy. All audit findings have been scrutinised and discussed with both the audit team and relevant senior management members. This allowed the Committee to assure itself that issues identified and the recommendations proposed were fair, proportionate and owned by the business.

11 Overall, the Committee is satisfied that there is a good control framework in place. The outcomes from individual reviews and the number of recommendations are shown in the following table.

Audit review		Assurance rating		Number of recommendations (high priority)
1	2016 IA follow up	Green		0
2	FTP s60 benefits realisation	Green-	amber	2 (1)
3	Digital media strategy – phase 1	Green	amber	7
4	Employer Liaison Service	Green	amber	6 (2)
5	Provisional enquiries	Green	amber	4
6	Contract management	Amber		10 (2)
7	MLA Phase 1	Amber		7 (3)
8	In House Legal Services	Green	amber	5
9	Use of experts	Green		3
10	Social media spot check	Green	amber	2
11	Change programme benefits realisation	Green	amber	3
12	COO dashboard and data integrity	Amber		10
13	Risk management in projects	Amber		8
14	Policy development and management	Amber		13 (5)
15	Expenses spot check	Green		3
16	ISO 27001	Green		4
17	Registration appeals	Green		1
18	Cross directorate service requests	Green	amber	5
19	Payroll	Green		1
20	Business planning	Green	amber	7
21	MPTS data accuracy and integrity	Green	amber	3 (2)
22	Curricula approvals	Green	amber	5
23	Enhanced monitoring follow up spo5t check	Amber		9 to be completed from 2016 (3)
	Total			**118 (18)**

12 Of the 118 recommendations made in the above reviews (which includes nine still be completed from the 2016 enhanced monitoring audit), 18 were high priority recommendations. These related to:

a Ensuring all the intended benefits from implementation of the S60 changes in FTP are captured and monitored in a single document.

b Taking a strategic look at the purpose of the Employer Liaison Service and developing a series of indicators and measures to capture information on the Service's impact.

c Giving further consideration to contract development and value for money through contract management.

d Taking steps to clarify the senior level leadership of the medical licensing assessment programme, reviewing resourcing requirements to support programme delivery and transferring the identified risks to a programme risk register for ease of scrutiny and oversight by the Programme Board.

e Taking steps to provide a clearer corporate strategic framework for the ownership, oversight, scrutiny and management of policy and policy development. (Much of this detailed work is already in hand alongside the restructuring of the new Strategy and Policy and Strategic Communication and Engagement directorates).

f Documenting standard procedures for producing management information in MPTS and introducing a formal quality assurance framework.

13 The spot check in relation to enhanced monitoring noted measurable progress, particularly in addressing the operational issues identified in the 2016 internal audit report. There has been investment in improving process and more rigour around decision making and some work has gone into understanding enhanced monitoring in the context of the regulatory framework which has helped clarify operational processes. To date three of the original eleven recommendations are fully implemented.

14 However, less progress has been made with respect to the strategic level direction supporting and underpinning enhanced monitoring which was a high priority recommendation in 2016. The Committee recognises that there is an important piece of work to do which will require Council's involvement. The Executive will be developing a seminar session to consider the issues with Council in due course. In the meantime the Committee will continue to oversee progress in implementing the recommendations raised through the recent audit work.

15 The Committee has also separately commissioned through the Assistant Director of Audit and Risk Assurance, an independent review of the GMC's BS 10008 (the British Standard for best practice in the implementation and operation of electronic information management systems) to which the GMC became fully accredited in 2016, and a review of cyber security.

16 The Committee noted that the GMC is one of the first few organisations to hold BS 10008 accreditation. The independent reviewer was complimentary about the work of the team concluding that the information management system at the GMC is effective in ensuring the trustworthiness of electronic information.

17 The cyber security review adopted a 'hacker' approach to make the work as realistic as possible to the increasing information security attacks we are noting in the media. This included two phishing tests, an increasingly common tactic used by hackers, both of which were identified quickly by the GMC's in-house security team. The report identified one high risk finding in relation to cross site scripting (where malicious scripts are injected in to a website application and sent to victims, for example by email, who open them and then pass the malicious script in to business systems) which has already been addressed by the IS Team. Overall the review concluded that in comparison to other organisations, the GMC is taking a proactive and mature approach towards cyber security.

18 At each meeting, the Committee has also received a progress report, including an update on the status of actions arising from internal audit work. There remains a continuing effort to close outstanding audit actions and the Committee is pleased to report that some of the longer standing recommendations that had taken longer to implement than anticipated are now closed, with the exception of enhanced monitoring. At the time of this report, with the exception of enhanced monitoring noted above, there are no recommendations overdue.

19 Finally, at its November meeting, the Committee considered a review of delegated authorities, which are set out in the Schedule of Authority and form part of the Governance Handbook. In particular, the Committee noted relevant amendments in relation to:

a The incorporation of GMC Services International.

b Decisions on the management of GMC funds and expenditure.

c MPTS and emphasising the separation of GMC investigations and MPTS adjudication functions.

Significant event reviews

20 Since the last report to Council the Committee has considered one significant event review (SER). It is satisfied that appropriate action was taken to address the event and appropriate learning and controls have been put in place where needed to mitigate as far as possible, a recurrence of the issue. The Committee noted a 'continuous improvement' style to drawing out the significant factors contributing to the SER. This was piloted to encourage a more open and facilitative learning approach in contrast to the more traditional investigative approach. On this occasion the pilot worked well and the use of the approach will be adopted for future SERs where it is considered appropriate.

Internal audit management arrangements

21 The Committee considers that the enhanced co-sourcing model continues to work effectively and the GMC has benefited from having carefully tailored audit scopes and the right level of expertise and knowledge delivering individual reviews. As last year, the Committee will be undertaking a formal evaluation of the performance of the internal audit function in the new year. The Committee has also contributed to a draft Internal Audit Strategy 2018-2020 which will sit alongside the Corporate Strategy. This is an important document which articulates audit's contribution in supporting the achievement of the GMC's purpose and corporate objectives.

Audit programme 2018

22 At its meeting in November, the Committee approved the audit programme for 2018. As in previous years, this will continue to feature all three types of audit review noted in paragraph 10 but adopting a more agile audit approach for areas of emerging risk where the Committee or Council need assurance. This will require the Executive and Committee to have more regular discussions throughout the year on where the areas of greatest risk and need for assurance are that audit work can be more targeted at a given point in time. The Committee has agreed the first areas of audit focus will be:

a GMC readiness to ensure compliance with the European General Data Protection Regulations which come in to force 25 May 2018.

b Preparations for phase 2 of the digital media strategy implementation.

c Arrangements to support delivery of the Transformation Programme.

The Committee's 2017 review of its effectiveness

23 The Committee will be undertaking it annual review of effectiveness during December 2017 and January 2018. As previously this will comprise a self-evaluation

questionnaire which will also be sent to the Executive and non-member attendees of the Committee, including external and internal audit. The Committee has chosen for its review seminar in January to hold a training session on unconscious bias, focused on bias in relation to risk, audit and assurance scrutiny.

Adding value

24 The Committee's role is to add value to the GMC through supporting the achievement of good governance. By continually improving its knowledge of the business and seeking assurance through audit and risk activity, the Committee believes it is improving its own performance and consequent value to the business through:

a Being clear on its role and purpose and continuing to check that this is still appropriate for the business's needs.

b Developing agendas and a programme of work which are pertinent to regular business and emerging issues so that meetings are relevant and focused.

c Holding regular seminars which focus on continual development of the Committee's knowledge and understanding of the business and specific risk areas.

d Providing scrutiny of the Corporate Risk Register.

e Holding management to account by calling directors and senior staff to meetings to respond to the findings from audit reviews and following through on the implementation of audit recommendations.

f Meeting internal and external auditors without management present.

g Regular dialogue between the Chair and Assistant Director of Audit and Risk Assurance between meetings.

h Dialogue between the Chair of Council and Chair of the Committee on emerging issues.

i Inviting auditors to provide broader insight from global and national risk and audit trends in the financial, political and health environments.

j Providing more time on agendas for reflecting on broader opportunity/risk issues and horizon scanning.