General Medical Council

Agenda item:	**9**
Report title:	**Report of the Audit and Risk Committee**
Report by:	**Lindsey Mallors**, Assistant Director - Audit and Risk Assurance lmallors@gmc-uk.org, 020 7189 5188
Considered by:	**Audit and Risk Committee**
Action:	**To consider**

Executive summary

This is the final report to Council for 2015 outlining the Audit and Risk Committee's assurance activities.

Key points to note are:

- The GMC has made good progress in rolling out the Risk Management Framework introduced in 2014 and successfully engaged staff at all levels of the organisation.
- Assurance can be provided on key controls across statutory directorate activities which have been subject to audit review.
- Management remains active in implementing recommendations arising from audit reviews.
- The Committee is satisfied with the performance of both the external and internal auditors.

Recommendation

Council is asked to note the Audit and Risk Committee's report.

Background

1 Since its last report to Council, the Audit and Risk Committee has met twice in formal session and seminar. Following changes the Committee made at the end of 2014, relevant directors, assistant directors or heads of sections have attended when audit reports relating to their area of business were being presented. This has proved valuable in providing an opportunity for members to challenge GMC colleagues on their areas of operation. It has also contributed to the Committee's assurance about the robustness of audit findings being suitable for the business, acceptance of findings and the ability of management teams to tackle issues identified.

2 At its meeting in November 2015 the Committee considered its Statement of Purpose, at Annex A, and believes that this remains relevant for its assurance role.

3 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

4 The work of the external auditors on the financial statements and Annual Report was reported to Council in June. Since then the Committee has undertaken its annual assessment of the performance of the external auditors, Crowe Clark Whitehill, which continues to be a positive one. Following a procurement process, the external auditors have been reappointed for a further three years.

Governance and risk management

5 The Committee uses a focus on risk as the basis for its approach to oversight scrutiny and review to be able to support the Council in making its statement in the Annual Report. It has played a proactive role in critically challenging the Corporate Risk Register at every meeting and undertaken detailed scrutiny of specific risks in seminar sessions.

6 An internal audit review was undertaken on the operational level of the Risk Management Framework (RMF), considering the effectiveness of risk management at directorate level and below. The Committee was pleased to note that the framework has been successfully introduced with appropriate engagement at all levels.

7 Risk management evolves over time in line with an organisation's maturity and the Executive are now leading an evaluation of the RMF to provide assurance that it is fit for future business and in line with the principles of effective risk management set out in the international guidance standard ISO31000:2009.

Systems of internal control

8 This year work on internal systems and controls has been completed with the new delivery internal audit partner, Moore Stephens. The audit programme was risk based and the Committee has welcomed the broader range of work undertaken which strengthens the overall assurance picture it has gained.

9 The programme is now complete for 2015 and the Committee has scrutinised all audit findings. Through the attendance of management at meetings, the Committee has satisfied itself that the actions proposed are appropriate and are assured that in general there is a good control framework in place. Annex B provides details of the individual reviews undertaken by internal audit.

10 There are two areas to draw to Council's attention. The review of quality assurance through regional visits confirmed that the visits for 2014 were carefully planned and a risk based approach was adopted with a degree of subjective judgement applied. However there are improvements needed to demonstrate at a strategic level how a comprehensive methodology driven risk based approach underpins the planning for regional visits. There is also a need to consider what escalatory regulatory sanctions/action could be used/developed within the existing legal framework to prompt visit sites to prioritise action follow up where the GMC considers progress is not acceptable.

11 The review of data and intelligence gathering and use was a substantial cross cutting piece of advisory work providing a useful stocktake for the organisation as well as some clear developmental recommendations. Importantly, the review concludes that the GMC has made good progress in this area and has a well-established, sophisticated process for evaluating risk to patient safety. The next key step is to define the purpose and scope of intelligence gathering and create the strategic framework and operational capability response to data gathering to support intelligence led regulation.

12 In addition to the specific audits, three spot checks were undertaken. There were no significant findings in the spot checks but some useful points were identified which have been addressed by management, including a refresh of the Gifts and Hospitality Policy which was circulated to Council members.

13 The Committee has also reviewed the implementation progress of audit actions and is pleased to report that actions are followed up in a timely manner.

Significant event reviews

14 Since the last update to Council, the Committee has reviewed three significant event reviews. These provide important learning opportunities and the Committee takes assurance from the actions management put in place as a result.

Audit and Risk Committee's annual review of its effectiveness

15 Following its review last year, the Committee developed an action plan which it has fully delivered during 2015 and this is reflected in the effectiveness review this year. Overall, there is a very high level of consensus amongst members and attendees (Executive and auditors who attend the meetings) on the effectiveness of the Committee.

16 As a result of this year's review, the Committee has agreed for 2016 that it will hold an additional two meetings. This will allow the presentation of audit reports in particular to be smoothed across the year and provide more time for detailed discussion of agenda items.

17 In addition the regular programme of seminars will continue providing the opportunity to explore areas of the business where the Committee considers further engagement with Executive colleagues and their teams would aid the effectiveness of its assurance role, including focused discussion on particular risk areas.

Performance of internal audit

18 The Audit and Risk Committee believes that there has been a transformation in the quality of internal audit in the last 18 months. This now performs at a very high level. Important topics are being addressed with due independence from management and high quality reports are produced. A strong working relationship has been established between the Head of Internal Audit, the external internal audit provider (Moore Stephens) and the external auditor (Crowe Clark Whitehill).

19 Informal feedback from the Executive, auditees and the auditors themselves is also encouraging and a formal evaluation of performance will be considered by the Committee at its meeting on 27 January 2016.

Assurance programme for 2016

20 After careful consideration, the Committee has now agreed its work programme for 2016. This maintains a risk based assurance approach and reflects emerging areas of challenge such as recognition of professional qualifications and implementation of the GMC Change Programme, including the potential effects on other business operations such as business continuity. In addition the Committee will continue to independently

commission assurance work on cyber security reflecting the continuing global concerns and increasingly frequently reported high profile cyber attacks.

Adding value

21 The Committee's role is to add value to the GMC through supporting the achievement of good governance. It believes it has achieved this through:

- Being clear on its role and purpose and continuing to check that this is still appropriate for the business's needs.
- Developing agendas which are pertinent to regular business and emerging issues so that meetings are relevant and focused.
- Providing scrutiny of the Corporate Risk Register and supporting risk management framework and undertaking 'deep dive' reviews of specific risk areas.
- 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.
- Meeting internal and external auditors without management present and regular dialogue between the Committee's Chair and Assistant Director of Audit and Risk Assurance between meetings.
- Commissioning a specific cyber security review on penetration testing through an independent supplier.
- Holding regular seminar sessions to give greater depth of background knowledge to members on key topics.
- Involvement in the procurement process for external audit services.

22 Finally, the Chair would like to record his thanks to Council and independent members of the Committee for their contribution and commitment throughout the year.

General Medical Council

M9 – Report of the Audit and Risk Committee

M9 – Annex A

Statement of Purpose of the Audit and Risk Committee

Purpose

1 The Audit and Risk Committee provides Council with independent assurances on the effectiveness of arrangements established by the Executive to ensure the:

a Integrity of the financial statements.

b Effectiveness of the systems of internal control, governance and risk management.

c Adequacy of both the internal and external audit services.

2 The Committee is specifically authorised by Council to:

a Investigate any activity within its terms of reference. Any investigation will normally be initiated in consultation with the Chief Executive.

b Seek any information it may reasonably require from any member, employee or associate. All members, employees and associates are directed to co-operate with any reasonable request made by the Committee.

c Obtain outside legal or other independent professional advice and to secure the attendance of people with relevant experience and expertise if it considers this necessary. The Committee may not incur direct expenditure in this respect in excess of its allocated budget without prior approval of the Chair of Council, in consultation with the Chief Executive.

Duties and activities

Financial Reporting

3 Review the annual financial statements taking into account advice from the external auditors and ensure they are a fair and accurate reflection of the activities of the GMC. If necessary, this should involve challenging the actions and judgements behind the

preparation of the annual financial statements and related documents, before submission to and approval by Council.

4 Review the organisation's accounting policies.

5 Consider any other topics, as directed by Council.

Internal Control and Risk Management

6 Monitor the integrity of internal controls. In particular, review management and the internal audit reports on the effectiveness of the system of internal control.

7 Assess the scope and effectiveness of the systems designed to identify, assess, manage and monitor significant risks.

8 Review statements in the annual report and accounts relating to audit and risk management.

9 Monitor anti-fraud policies and procedures and review arrangements for raising concerns.

10 Review all delegated authorities at least once in every four-year Council term.

Internal Audit

11 The appointment or dismissal of the Assistant Director of Audit and Risk Assurance and the external provider of internal audit services is the responsibility of the Chief Operating Officer in consultation with the Chief Executive, but should be ratified by the chair of the Audit and Risk Committee. In the event of any unresolved disagreement between the Chief Executive and the chair of the Committee, the matter will be referred to the Chair of Council.

12 Ensure that the Assistant Director of Audit and Risk Assurance has direct access to the Chair of Council and the Committee and is accountable to the Committee.

13 Review the internal audit programme and ensure that the function is adequately resourced and has appropriate standing within the organisation.

14 Consider and monitor the organisation's response to any major internal audit recommendations.

15 Monitor and assess the role and effectiveness of the internal audit function.

16 Ensure the provision of any non-audit services does not impair the internal auditors' independence or objectivity.

External Audit

17 Consider and make recommendations to Council on the appointment, reappointment and removal of the external auditors.

18 Approve the terms of engagement and fee to be paid to the external auditor in respect of audit services provided.

19 Assess the qualification, expertise, resources, effectiveness and independence of the external auditors annually.

20 Discuss in advance with the external auditor the nature and scope of the audit.

21 Review with the external auditors their findings, the content of the management letter and management's responses and the audit representation letter.

22 Ensure the provision of any non-audit services does not impair the external auditors' independence or objectivity.

Working arrangements

23 Meetings will be held at least four times a year. At the discretion of the chair of the Committee, additional meetings can be convened.

24 The Committee should review its statement of purpose at least once a year and suggest any necessary amendments to Council.

25 The external auditors or internal auditors may request a meeting of the Committee.

26 At least once a year the Audit and Risk Committee should meet the external auditors and internal auditors without management.

27 Members of the Committee (including the co-opted members) may meet alone at any time. Normally, senior staff will be in attendance including the Chief Executive, the Chief Operating Officer, the Director of Resources and Quality Assurance, the Assistant Director of Finance and Procurement, and the Assistant Director of Audit and Risk Assurance. Others may attend meetings at the invitation of the Committee.

28 Draft minutes should be cleared by the chair and circulated to members for comment within two weeks of the meeting. Minutes are circulated to all Council members.

29 Where the Committee is not satisfied with any aspects of the organisation's performance in relation to audit and risk or other systems of internal control it will report its views to Council.

30 The Committee prepares a report, for inclusion in the annual report and accounts, on its role and responsibilities and the actions it has taken to discharge those

responsibilities. The report includes any unresolved disagreements between Council and the Committee.

31 The chair or another designated member of the Committee, if the chair is not available, presents a report and answers questions on the Committee's activities for Council at least twice a year.

General Medical Council

M9 – Report of the Audit and Risk Committee

M9 – Annex B

Overview of the internal audit programme reviews

1 The audit ratings for each review are based on a five-point scale of green through to red. The table below outlines each review under the level of assurance provided by the rating. There were no reviews with either amber/red or red assurance ratings.

Green Overall, there is a sound control framework in place	**Green/amber** Minor weaknesses have been identified	**Amber** Weaknesses have been identified
■ Integrity/accuracy of HR management information ■ MPTS systems compliance ■ Procurement systems compliance ■ UK applications system compliance ■ Financial controls ■ Business continuity	■ Public interest and disclosure arrangements ■ Risk management ■ Performance appraisal arrangements ■ ISO27001/BSI10008 review ■ Fitness to practise compliance ■ Monitoring of sanctions ■ Data strategy *	■ Education Regional visits quality assurance compliance ■ Data and intelligence gathering and use/working with others *

* Included in the programme as advisory reviews with a development focus

2 In addition, cyber security penetration testing was undertaken, commissioned by the Committee through an independent supplier. This work did not award ratings but provided a number of recommended actions, none critical and all accepted by management.