

Internal audit charter and protocol
The University's responsibilities and its arrangements for internal audit
2017/18 to 2019/20

Summary

This paper sets out the University's current obligations and arrangements for internal audit, and formally establishes the purpose, authority and responsibilities of the Internal Audit function. It also defines the processes and requirements that govern the internal audit process during the period of the internal audit contract for the years 2017/18 to 2019/20.

Internal audit

Internal audit is an independent, objective assurance and consulting activity designed to add value and improve an organisation's operations. It helps an organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluating and improving the effectiveness of risk management, control and governance processes.

The internal audit protocol 2017/18 to 2019/20

This internal audit protocol has been developed to set out clearly the responsibilities of the internal auditors and the audited units¹, and to define the responsibilities, timetables and processes that govern the internal audit process - see Parts A-F of this document.

HEFCE's requirements for internal audit and assurance

Under the terms of the 'Memorandum of assurance and accountability between HEFCE and the University'², Council must ensure that it is fulfilling its responsibilities to ensure that the University has a robust and comprehensive system of risk management, control and corporate governance; and that it uses public funds for proper purposes and seeks to achieve value for money from public funds. Council must also ensure that it has effective arrangements for the management and quality assurance of data submitted to HESA, the Student Loans Company, HEFCE and other funding bodies.

The responsibilities of Council

Responsibility for these arrangements remains fully with Council, and Council seeks assurance on these matters from the Audit and Scrutiny Committee.

The responsibilities of the Audit and Scrutiny Committee

The Audit and Scrutiny Committee is responsible under Annex A to the Memorandum of assurance and accountability, the 'Audit Code of Practice', for assuring Council about the adequacy and effectiveness of the following areas:

- i. risk management;
- ii. control;

¹ In this regard, 'audited units' refers to the units of the University being audited, to include academic divisions, departments, faculties and research centres, administrative and service departments, subsidiaries and other auditable units.

² hefce.ac.uk/reg/MAA/

- iii. governance;
- iv. Value for Money ('VFM'); and
- v. the management and quality assurance of data.

The Committee reports annually to Council on its opinion as to the adequacy and effectiveness of the University's arrangements for these five areas.

The Audit and Scrutiny Committee's opinions on these arrangements are based on the information presented to the Committee. This includes (but is not confined to) evidence presented by the University's internal auditors, whose annual reports include an opinion on the five elements above. Internal audit is designed to provide "reasonable assurance" in relation to these areas, and cannot provide any guarantee against material errors, loss or fraud.

The University's internal audit function

The University's internal audit function is provided by an external firm, PricewaterhouseCoopers LLP ('PwC'), under a directed outsourcing arrangement, currently a three-year contract from 2017/18 to 2019/20. While the internal auditors are external to the University, the planning, delivery and reporting of their work is supervised by the Audit and Scrutiny Committee. All of the University's activities (including outsourced activities) and legal entities are within scope of Internal Audit (except for the Press).

The internal audit plan is developed in collaboration with, and is approved by, the Audit and Scrutiny Committee, and adopts a risk-based approach to focus audit work on the Committee's priorities and the key risks facing the University.

The Audit and Scrutiny Committee will be updated regularly on the work of the internal auditors through periodic and annual reports. Reports of audit activities will include significant findings along with any relevant recommendations and provide periodic information on the status of the annual audit plan.

Internal Audit does not necessarily cover all potential scope areas every year. The audit program includes obtaining an understanding of the processes and systems under audit, evaluating their adequacy, and testing the operating effectiveness of key controls. Internal Audit can also, where appropriate, undertake special investigations and consulting engagements at the request of the Audit and Scrutiny Committee.

In order to be effective, the internal auditors have access to the Chair of the Audit and Scrutiny Committee, the Vice-Chancellor, the Registrar and other senior officers as necessary. In addition, departments and other units that receive visits from the internal auditors are required to assist them in the scoping, planning and delivery of their audit work so that the resulting report is of maximum possible value both to the audited unit and to the Committee in the development of its annual opinion.

Responsibilities of the Head of Internal Audit

The Head of Internal Audit (who is the PwC Engagement Partner) is responsible for preparing the annual audit plan in consultation with the Audit and Scrutiny Committee, the University members of the Audit Management Group and senior management, submitting the audit plan, internal audit budget, and resource plan for review and approval by the Audit Management Group and the Audit and Scrutiny Committee, implementing the approved audit plan, and issuing periodic audit reports on a timely basis to the Audit Management Group and the Audit and Scrutiny Committee and senior management.

The Head of Internal Audit is responsible for ensuring that the Internal Audit function has the skills and experience commensurate with the risks of the organisation. The Audit and Scrutiny Committee should make appropriate inquiries of management and the Head of Internal Audit to determine whether there are any inappropriate scope or resource limitations.

Responsibilities of management

It is the responsibility of management to identify, understand and manage risks effectively, including taking appropriate and timely action in response to audit findings. It is also management's responsibility to maintain a

sound system of internal control and improvement of the same. The existence of an Internal Audit function, therefore, does not in any way relieve them of this responsibility. Management is responsible for fraud prevention and detection. As Internal Audit performs its work programs, it will be observant of manifestations of the existence of fraud and weaknesses in internal control which would permit fraud to occur or would impede its detection.

Responsibilities of the Audit Management Group

The Audit Management Group is responsible for the management and monitoring of the internal audit contract on behalf of the Audit and Scrutiny Committee. Membership of the Group is given in Part E. Members are drawn from the University and the internal auditors. In terms of its internal audit work, the Group oversees the preparation of the annual internal audit plan, for approval by the Audit and Scrutiny Committee. It monitors the progress of audit work and coordinates reporting to the Audit and Scrutiny Committee. It also manages the follow-up of internal audit recommendations (see Part C). The University members of the Group consider questions relating to the independence and objectivity of the external and the internal auditors (see Part D).

Contact details

The relationship with the internal auditors is managed by the Head of Assurance and Risk Management on a day-to-day basis. Colleagues are invited to contact the Head of Assurance and Risk Management to discuss any concerns they may have with internal audit, or to raise areas requiring investigation (sally.vine@admin.ox.ac.uk, (2)80179).

Part A: process, timetable and reporting

These processes and timescales are indicative and may be altered with the agreement of the auditable unit, the internal auditors and the Head of Assurance and Risk Management. Some audit work will not fit easily into this outline timetable and a flexible approach will need to be adopted. In circumstances where agreement cannot be reached, the Audit Management Group will set out the timescale that will be required.

Process	Responsible	Timescale (these timescales are indicative only and are subject to change)
Audit planning		
Sponsor identified and consulted. Sponsors and internal auditors to identify and agree the purpose of the review, its place in the current year's internal audit plan and the assurance framework, the risks addressed by the work, and the intended outcomes and deliverables.	Internal auditors and sponsors; also Head of Assurance and Risk Management and AMG consulted.	By end of January.
Draft Terms of Reference issued, confirming key audit milestone dates for the fieldwork and reporting stages of the audit.	Internal auditors	No less than 2 weeks before the start of audit fieldwork.
Comments provided on draft Terms of Reference	Head of Assurance and Risk Management and Audit Sponsor(s)	No less than 1 week before the start of audit fieldwork.
Final Terms of Reference issued and approved	Internal auditors; Head of Assurance and Risk Management and Audit Sponsor(s)	Before the start of fieldwork.
Audit fieldwork and closure		
Closing meeting to confirm matters arising from the audit.	Internal auditors and sponsors/departmental audit contacts as appropriate.	Last day of field work, or no more than 2 weeks after completion of fieldwork.
Audit reporting – initial draft		
Initial draft audit report issued to stakeholders. Report graded if appropriate (see Part C: internal audit report grading).	Internal auditors	As soon as possible after closing meeting; timescale will depend on the nature of the report, but no more than 2 weeks after closing meeting.
Confirmation as to the material accuracy of the initial draft report and highlighting of issues to be discussed/ amended.	Head of Assurance and Risk Management	As soon as possible; will depend on nature of report

	to receive initial draft for comment. Followed by Audit Sponsors/departmental audit contacts as appropriate	but no more than 2 weeks after receipt of draft.
Management responses (where required)		
Sponsors/departmental audit contacts provide (where the reporting format requires): (i) management responses to individual audit recommendations, including responsible officers for implementation and deadlines; (ii) overall conclusion for the executive summary of the report.	Sponsors/departmental audit contacts as appropriate.	This will happen at the same time confirmation of material accuracy of the initial draft report occurs (within 2 weeks of receipt of draft report). Infrequently, it may be identified at the fieldwork closing stage or whilst confirming factual accuracy that more time is required to provide management responses.
Internal auditors confirm the management responses, proposed delivery dates and responsible officers as acceptable for audit purposes and issue final draft report.	Internal auditors	No more than 2 weeks after receipt of management responses.
Final draft report		
Sponsors/departmental audit contacts confirm final draft report.	Sponsors/departmental audit contacts Internal auditors Head of Assurance and Risk Management	No more than 1 week after final draft report has been issued.
Final report		
Report re-graded if appropriate (see Part C: internal audit report grading). Final report circulated.	Internal auditors	Within 1 week of departmental confirmation of final draft
Post-audit recommendations		
Audit recommendations tracked and departments provide evidence as recommendations are completed.	Departmental contacts Head of Assurance and Risk Management Internal auditors	According to timing of individual recommendations.

Part B: post-audit recommendation tracking and extensions

Once an internal audit report has been finalised, any recommendations must be acted upon within the agreed timescale. This process will be managed by the Head of Assurance and Risk Management who will work with the internal audit team and the audited units to ensure that recommendations are completed and evidenced. In exceptional circumstances, the audited unit may need to seek an extension to the completion date. Extensions will be managed by the Head of Assurance and Risk Management, and reported to the Audit Management Group. If the extension cannot be agreed, the Head of Assurance and Risk Management will refer the issue to the Audit Management Group for resolution. In the event that the Audit Management Group cannot reach a satisfactory resolution, the matter will be referred to the Chair of the Audit and Scrutiny Committee, and/or to a meeting of the Committee.

Departmental audit contacts are asked to note that it is essential that recommendations are discussed and understood as they arise during the fieldwork stage, at the completion meeting, and during the report drafting process. Full engagement in the process of developing the audit recommendations should ensure that the failure to address a recommendation by the deadline only occurs in exceptional circumstances.

Part C: internal audit report grading

Internal audit findings are given a risk rating in order to indicate the severity of the findings and to prioritise management action to address recommendations. Internal audit reports are also given an overall rating to indicate the severity of the findings in the report. The system is applied to all internal audit reports and will be reviewed regularly to ensure that it remains appropriate.

i. Findings ratings

A finding is a control failure, instance of non-compliance, or other matter identified during a review that requires, in the judgement of the internal auditors, reporting to management. Findings generally give rise to audit recommendations, require management responses, and are tracked to ensure that corrective action has been taken.

Findings may be reported in formal audit reports, letters or other forms of reporting, but whatever the form of the report, the findings identified will have a formal rating attached, to facilitate tracking and management action. All findings will be tracked unless specific exceptions are made.

Ratings will be defined for findings identified during a review. Findings are assessed on their impact and likelihood based on the assessment rationale in the tables below. Findings might be material for the unit under review, but not material in the context of the University as a whole

Table 1: Impact assessment rationale

Impact is considered across the following dimensions:

- operational performance;
- monetary or financial statement impact;
- breach in laws and regulations that could result in material fines or consequences; and
- the reputation or brand of the University/unit which could threaten its future viability.

Impact rating	Assessment rationale
6	A finding which is indicative of control failure, weakness or non-compliance, that could have a critical impact on the University's ability to achieve strategic or operational objectives and is material to the unit under review.
5	A finding which is indicative of control failure, weakness or non-compliance, that could have a significant impact on the University's ability to achieve strategic or operational objectives and is material to the unit under review.
4	A finding which is indicative of control failure, weakness or non-compliance, that could have a major impact on the University's ability to achieve strategic or operational objectives and is material to the unit under review.
3	A finding which is indicative of control failure, weakness or non-compliance, that could have a moderate impact on the University's ability to achieve strategic or operational objectives and is material to the unit under review.
2	A finding which is indicative of control failure, weakness or non-compliance, that could have a minor impact on the University's ability to achieve strategic or operational objectives and is not material to the unit under review.
1	A finding which is indicative of control failure, weakness or non-compliance, that is restricted to but not material to the unit under review.

Advisory	A finding that does not have a risk impact but has been raised to highlight areas of inefficiencies or good practice.
-----------------	---

Table 2: Likelihood assessment rationale

Likelihood rating	Assessment rationale
6	Has occurred or probable in the near future
5	Possible in the next 12 months
4	Possible in the next 1-2 years
3	Possible in the medium term (2-5 years)
2	Possible in the long term (5-10 years)
1	Unlikely in the foreseeable future

Once impact and likelihood ratings are determined for each finding, an overall finding rating can be derived – see table 3. There are four finding ratings: critical (RED); significant (AMBER); medium (YELLOW) and low (GREEN).

Table 3: Consolidating severity and scale dimensions to give an overall issue rating

Likelihood rating	Impact rating					
	6	5	4	3	2	1
6	Critical	Critical	High	High	Medium	Medium
5	Critical	High	High	Medium	Medium	Low
4	High	High	Medium	Medium	Low	Low
3	High	Medium	Medium	Low	Low	Low
2	Medium	Medium	Low	Low	Low	Low
1	Medium	Low	Low	Low	Low	Low

ii. Report ratings

Some reports will also have a rating, but not all. Some, such a real-time reporting on IT programmes, or brief letters, will have findings ratings but not a report rating.

Report ratings should arise from findings ratings, so as to avoid subjectivity or difficulty in agreeing a report rating. The report classification is determined by allocating points to each of the findings included in the report as set out in tables 4 and 5.

Table 4: Findings rating

Findings rating	Points
Critical	40 points per finding
High	10 points per finding
Medium	3 points per finding
Low	1 point per finding

Table 5: Report classification

Report classification	Points
● Satisfactory	6 points or less
● Satisfactory with exceptions	7 – 15 points
● Needs improvement	16 – 39 points
● Unsatisfactory	40 points and over

Publication of reports according to report rating will follow the model in table 6, whereby “unsatisfactory” reports are reported to Council and the summaries of all other reports bearing a report rating are posted on the intranet.

Table 6: Report circulation according to report rating

Report rating	Report circulation
Unsatisfactory	Council will be included in final report distribution (including appendices) following approval from Audit and Scrutiny Committee.
Needs Improvement	Report Executive Summary posted on the University intranet, following approval from the Audit and Scrutiny Committee.
Satisfactory with exceptions	Report Executive Summary posted on the University intranet, following approval from the Audit and Scrutiny Committee.
Satisfactory	Report Executive Summary posted on the University intranet, following approval from the Audit and Scrutiny Committee.

Part D: processes designed to protect the independence and objectivity of the internal auditors

An important element of good governance is the independence and objectivity of the external and the internal auditors. The provision of any non-audit related services to the University by the external or the internal auditors, or the provision of any services (courses, training, consultancy or other academic services) to the external or the internal auditors by the University or any member of University staff must not compromise this independence and objectivity. Philanthropic support or sponsorship must only be accepted from the external or the internal auditors where it does not affect, or cannot be perceived to affect, the auditors' independence and objectivity.

The Policy to Safeguard the Independence of the External and the Internal Auditors³ sets out the University's objectives for protection of the independence of the external and the internal auditors, and the arrangements it has adopted to enable it to safeguard the independence of the audit firms engaged by the University.

Internal Audit staff will remain independent of the University and they shall have no direct operational responsibility or authority over any of the activities they review. Therefore, they shall not develop nor install systems or procedures, prepare records or engage in any other activity which they would normally audit. Internal Audit staff with real or perceived conflicts of interest must inform the Engagement Partner, then the Audit Management Group, as soon as these issues become apparent so that appropriate safeguards can be put in place.

The Internal Audit function will perform its duties with professional competence and due care. Internal Audit will adhere to the Definition of Internal Auditing, Code of Ethics and the Standards for the Professional Practice of Internal Auditing that are published by the Institute of Internal Auditors.

Colleagues wishing to engage the internal auditors for the conduct of non-audit work, or to supply any academic services to the internal auditors, or to accept gifts or sponsorship from the internal auditors, are asked to contact the Head of Assurance and Risk Management in the first instance (sally.vine@admin.ox.ac.uk, (2)80179).

³ admin.ox.ac.uk/iso/statutes/policyonauditorsindependence/

Part E: the Audit Management Group: membership

Registrar, Professor Ewan McKendrick (chair)

Director of Finance, Giles Kerr

Deputy Director of Finance, Lindsay Pearson

Head of Assurance and Risk Management, Sally Vine

Engagement Partner, PwC, Geraldine Rutter

Senior Manager, PwC, Sophia Mouyis

Secretary: Administrative Officer (Assurance and Risk Management), Sophie Hockley

Questions or concerns regarding internal audit should be directed to Sally Vine, on (2)80179 or sally.vine@admin.ox.ac.uk.

Part F: Operation of 'Part C' of the internal audit contract

Part C of the internal audit contract allows for the ability for the internal auditors to respond to events or management requests that cannot be accommodated by adjusting the internal audit plan. These additional pieces of assurance work are funded by the department or function requesting the work. Any work sourced by this method will be reported to the Audit and Scrutiny Committee.