THE UNIVERSITY OF MANCHESTER

AUDIT AND RISK COMMITTEE (by video conference) 31 March 2022

Present: Deirdre Evans (Chair)
Ann Barnes
Robin Phillips
Trevor Rees

Apologies: Alice Webb
Alex Creswell (advisor to the Committee)

In attendance: Patrick Hackett, Registrar, Secretary and Chief Operating Officer (RSCOO)
John Cunningham, Interim Chief Financial Officer
Dr David Barker, Director of Compliance and Risk
Richard Young, Uniac
Sue Suchoparek, Uniac
Alastair Duke, PKF Littlejohn
Angus Hearmon, Director of IT Services (item 7only)
Tony Brown, Head of Information Governance (item 7 only)
Pete Bradley, Identity and Security Manager-IT Services (item 7 only)

Secretary: Mark Rollinson, Deputy Secretary

1. Declarations of interest

Noted: there were no new declarations of interest.

2. Minutes

Resolved: that the minutes of the meeting held on 26 January 2022 be approved.

3. Matters arising and action tracker

Received: the action tracker setting out progress against matters arising from earlier meetings. A further progress report on the issue of staff overpayments was covered in the report from Uniac.

Noted: a date would be agreed for updating of policies (item 8 in the report).

Action: Deputy Secretary

4. Membership

Reported: Erica Ingham had resigned as a co-opted member of the Committee.

5. Internal Audit and Internal Control

(i) Uniac Progress Report

Received: the latest Uniac internal audit progress report, which contained a summary of audits finalised since the previous meeting of the Committee, an update on assurance mapping, and progress to date against the agreed action plan.

(a) Staff Overpayments (Follow up)

Reported:

(1) Following the request at the previous meeting of the Committee, Uniac had undertaken further follow-up work in relation to staff overpayments.

(2) Based on this work, Uniac concluded that there had been significant progress, with repayments happening on a timely basis, communication amongst relevant staff had improved and processes in place were more robust than those observed elsewhere in the sector.

(3) Given scale and complexity of the University and current systems limitations, it was not possible to entirely eradicate staff overpayments. However, no systemic issues had been identified and recent overpayments had occurred for a variety of one-off reasons.

(4) The previous decision of the Committee to write off all debt over two years old had not yet been fully implemented and Uniac recommended that this be completed as soon as possible as this would significantly reduce the balance on the overpayments account enabling focus on current issues.

(5) Uniac endorsed the recommendation to set a threshold of 0.1% of both the rate of overpayment of total staff paid and of the rate of total overpayments against the monthly pay bill: if either of these KPIs were exceeded, a report to the Committee would be triggered, including explanation for the variance.

Agreed: to support the 0.1% threshold as outlined above and that, additionally, a report be triggered by any significant one-off overpayment. **Action: Director of People and OD**

(b) Health Education England: contract management

Reported:

(1) Following an earlier review (in 2020) and given the nature and complexity of Health Education England (HEE) funding provision and requirements for effective contract management and oversight, a review of processes and controls for HEE contracts was undertaken.

(2) The report provided limited assurance in relation to effectiveness of design with instances of some contracts receiving approval without appropriate oversight by University legal, contract and finance teams. In addition, there was a lack of both documented end to end process for HEE contract management and of financial viability assessment for ongoing HEE contracts.

(3) Agreed management action to address these matters was set out in the report with commitment to full end to end review of HEE contracting to be completed and rolled out for the beginning of academic year 2023-24. Areas of good practice were also found and highlighted in the report.

Noted:

(1) The Committee asked to be kept apprised of the progress of the end to end review.

Action: Deputy Secretary

(2) The importance of establishing a culture with expectations about compliance (and potential consequences for non-compliance) and of regular review and challenge of established practice.

(c) Access and Participation Plan

Reported:

(1) The report followed an earlier review from July 2020 and aligned with sub-risk 4.2 of the Strategic Risk Register (failure to provide a high-quality teaching, learning and co-curricular experience). It focused on approaches taken to promote the Access and Participation Plan (APP) and its targets and the use of data and how resources are used and accounted for in narrowing unexplained gaps in student outcomes.

(2) The review provided reasonable assurance in relation to effectiveness of design, effectiveness of implementation and economy and efficiency and outlined management action to address four moderate risk findings, noting the need to embed a defined and systematic approach to tacking unexplained student outcomes.

(d) Human Tissue Act Compliance

Reported:

(1) The purpose of the audit was to provide independent assurance that the University had effective and efficient controls and quality assurance processes to ensure compliance with the Human Tissue Act under its research licence and also considered the response to an issue of non-compliance reported to the Committee the previous year.

(2) The review provided reasonable assurance in relation to effectiveness of design, effectiveness of implementation and economy and efficiency and outlined management action to address three moderate risk findings (and the potential to address this further via actions targeting the source of non-compliance). The annual Research Compliance Committee report to the Committee provided further assurance in this area.

Agreed: the Committee be updated on the reply from the Human Tissue Authority to the University's response on the issue of non-compliance.

Action: Research Governance, Ethics, and Integrity Team

(e) Institutional Change Programme

Reported:

(1) The review had been requested by the Chair of Finance Committee and considered adequacy of financial information and risk reporting, approval processes relating to the overall Institutional Change Programme and related approval, delegation and authorisation matters (considering the roles and responsibilities of key governance bodies, i.e, Board of Governors, Finance Committee, Planning and Resources Committee)

(2) The report noted that work in this area continued to evolve (noting the significant progress made in the development of the Institutional Change Programme since the establishment of the Strategic Change Office in 2019) and accordingly the review was advisory without an overall assurance rating.

(3) Areas for potential further development included improving the Strategic Change dashboard to capture delivery of benefits more comprehensively and ongoing work on the Scheme of Delegation to provide greater clarity on Board and Finance Committee financial authority levels

Noted: further discussion would take place between the Chairs of Finance and Audit and Risk Committee to ensure clarity and complementarity in relation to the work of the committees (noting ongoing work on updating terms of reference).

(f) UUK Accommodation Code of Practice Compliance-University Halls

Reported:

(1) The review assessed University compliance with the UUK Accommodation Code of Practice for the Management of Student Housing across a sample of University halls of residence.

(2) The review provided substantial assurance in relation to effectiveness of design, and reasonable assurance in relation to effectiveness of implementation and economy and efficiency.

(g) UUK Accommodation Code of Practice Compliance-Private Halls

Reported:

(1) The review assessed University compliance with the UUK Accommodation Code of Practice for the Management of Student Housing in privately owned halls.

(2) The review provided reasonable assurance in relation to effectiveness of design, effectiveness of implementation and economy and efficiency.

(h) Tracker/Post Audit Review Exercise

Reported:

(1) The latest update tracking implementation of agreed actions from Uniac reports.

(2) There had been considerable management effort to ensure actions were being progressed with effective liaison with colleagues in faculties and professional services (and follow-up from Uniac to independently check validity of entries and test if necessary).

(3) The review provided substantial assurance in relation to effectiveness of design, and reasonable assurance in relation to effectiveness of implementation and economy and efficiency, noting that the University's reported level of compliance was exemplary.

(i) Assurance Mapping

Reported:

(1) Uniac had continued with its assurance mapping exercise, considering all of the risks from the risk register, working with risk owners and risk managers.

(2) Work included further articulation of both risks and sub-risks, and related mitigations and confirming three lines of assurance/defence.

Noted:

(1) Related detailed work was set out in the Diligent Reading room and this indicated that the University's position in relation to risk assurance was at a relatively mature stage compared to peers in the sector.

(2) A recent Uniac event had been attended by a senior representative of the Office for Students (OfS) who had advised that there was an expectation that institutions develop assurance maps. The University's relatively advanced position meant that it was well placed to contribute to planned OfS project/pilot work in this area.

(3) The nature and description of some risks impacted on the assurance process

(4) Risk assurance maps will be used to develop and inform the 2022-23 internal audit programme.

(5) The need to consider future ownership of the process (e.g. embedding outputs within relevant directorates, for use by relevant staff).

(ii) UKRI Funding Assurance Programme: Follow-Up

Received: a report providing an update on the status of the action plan established to address the findings of the UKRI Funding Assurance audit: further updates would be provided to the Committee until UKRI had confirmed all actions were completed and the Limited Assurance rating removed.

Noted: UKRI had advised that it was satisfied with levels of engagement and progress made to date.

(iii) Summary of Internal Investigatory Work

Received: a summary of internal work undertaken in relation to suspected frauds and irregularities since January 2022.

Noted: the Committee would be updated further on the suspected credit card and gift voucher fraud at its next meeting. **Action: Chief Financial Officer**

6. External Audit

Received: a brief, verbal update from PKF Littlejohn on progress on the external audit.

7. Strategic Risk Register

Received:

(1) The current iteration of the Risk Register and the covering report considered by the Board of Governors at its meeting on 22 March 2022.

(2) A presentation covering Risks 1.1 (Major Incident related to Cyber Risk) and 1.2 (Major Regulatory Incident related to Information Security and Data Protection) and a report on Cyber Risk considered by the Board of Governors at its meeting on 22 March 2022.

Reported:

(1) Between July and December 2021, the Information Commissioner's Office recorded 1,345 cyber-security incidents, a 20% year-on-year increase.

(2) Risk 1.1 (major incident related to cyber risk) had undergone some updating since the version of the Risk Register referred to in above (and this update was appended to the report) and there would be a full review of risk and mitigating actions (informed by work from Uniac) to inform the next iteration of the Risk Register in June 2022.

(3) An update on University preparedness, including response plan, exercises, communications plans and links to the National Cyber Security Centre.

(4) The current state of the cyber environment (e.g network, data centres, firewalls, remote connectivity) noting some areas of local vulnerability (e.g local servers not centrally controlled and susceptible to malware).

(5) Recent improvement in the University's BitSight (cyber security rating) score: this was the result of a number of actions, including implementation of "Default Deny" to restrict accessibility of computers on the network from the internet.

(6) Recent activity, including introduction of multi-factor authentication for students and activities on the related risk (1.2, Information Security and Data Protection): the latter included risk mitigation and information security classification

(7) Contingency planning and emergency response exercises were contributing to increased University resilience and preparation for cyber-breach, and it was essential to ensure continued vigilance and awareness (noting the importance of individual behaviour). Effective communications and awareness raising were essential elements in combatting individual susceptibility to cyber-attacks (e.g. Phishing exercises).

(8) In a research based university it was important to ensure an appropriate balance between central control and individual responsibility (noting that this environment and culture meant that there were vulnerabilities not applicable in other sectors).

(9) Whilst it was not possible to obtain relevant insurance in the current environment (given, for example, prevalence of malware attacks in the sector), there were ongoing discussions about access to specialist external remediation services if required.

(10) Planned activities, noting the continued need to upgrade and develop as the threat evolved (in this context, the University's recent rapid response to address a potential vulnerability, after it had emerged at another University was noted).

Noted:

(1) Given the likelihood and impact of the risk, the importance of a clear, prioritised timeframe for action.

(2) The evolving nature of the threat meant that there would always be a level of residual risk: the presentation and discussion showed that the University was tackling this in a structured and robust manner, supported by significant investment (£5 million in the current financial year).

(3) The importance of heightened awareness of the threat amongst staff so that they were sufficiently forewarned and equipped to take necessary preventative action: in this context, it was important to engender a sense of collective responsibility for protection of data.

(4) There had been limited time to consider emerging risks (noting some discussion of this at the Board meeting in the previous week): there had been some discussion of this between members before the meeting and this would be fed into the RSCOO and Director of Compliance and Risk.

(5) Currently, the Register was updated formally twice a year and it was important to ensure that this process allowed for timely consideration of exceptional issues and rapidly emerging risks to ensure that these were addressed in a timely way.

Agreed: Given the prominence and potential impact of the cyber risk, the Committee continue to receive regular updates and that this include timescales and planned prioritisation (ensuring emphasis on activities that will have the greatest impact).

Action: RSCOO and Director of IT Services

8. Public Interest Disclosures

Noted: there had been no Public Interest Disclosures since the previous meeting.

9. Dates of remaining meeting in 2021-22

Noted: the next meeting was on 15 June 2022 at 10.00am.