THE UNIVERSITY OF MANCHESTER

AUDIT AND RISK COMMITTEE (by video conference) 20 May 2021
Unconfirmed

Present:	Mr Colin Gillespie (Chair) Mrs Ann Barnes Ms Erica Ingham Mr Robin Phillips Mrs Alice Webb
Apologies:	Mr Trevor Rees
In attendance:	Chair of the Board of Governors Registrar, Secretary and Chief Operating Officer (RSCOO) Deputy Director of Finance Director of Compliance and Risk Director of IT (from item 2 ii) Director of Human Resources (from item 2 ii) Director of Planning (from item 2 ii) Head of Information Governance (from item 2 ii) Director, Student Recruitment and International Development Mr Richard Young, Uniac
Secretary:	Deputy Secretary

1. Declarations of interest

Noted: there were no new declarations of interest.

2. Risk

Received: the latest iteration of the Risk Register.

i) Initial discussion of the latest iteration of the Risk Register: exploring overall and relative position of risks

Noted:

(1) The latest iteration of the Risk Register had been subject to review by senior management and discussion with Risk Managers and Risk Owners to ensure greater consistency. Members recognised the extent and value of work undertaken to improve the maturity of the Risk Register and this had resulted in a greater spread of risks: there was recognition that there was still some variability in the maturity of risk description. The key data box for each risk contained a mixture of qualitative and quantitative information, with some areas needing further development.

(2) The importance of ensuring that:

a) senior management fully owned the Risk Register and good progress had been made in this regard recently:

b) there was a clear focus on mitigation:

c) there was greater specificity in risk description (for example there was similarity in risks 5 and 6 (minutes 2 iv) and 2 v) below) and this would benefit from further attention and review).

(3) Individual risks would benefit from an articulation of the desired end state and additional capability required to achieve this: this was linked to risk appetite and toleration.

(4) The Board Strategy Meeting on 5 July includes a session on Risk Appetite: it was important for the Committee and the Board to understand broader risk context and environment and the summary page at the front of the Register would benefit from a summary outlining this, to be updated iteratively.

(5) Scheduling of future Committee meetings should provide detailed analysis of one or two of the most significant, specific risks at each meeting, with periodic overview and assessment of the full Register.

ii) Consideration of the top six risks on the Register

(The Committee considered the top six risks on the Register in turn, with specific Risk Managers in attendance.)

a) Major Incident related to Cyber and related risk

Noted:

(1) A number of Universities had recently been subject to ransomware attacks and such incidents posed significant financial, operational and reputational risks. The cyber-threat landscape was evolving continually with potential risk from a range of actors, including criminals, disgruntled employees and nation state sponsored groups.

(2) An assessment of current key mitigations was outlined in the report, but in broad terms these were a mixture of improving control measures (for example, multi-factor authentication for students as well as staff) and encouraging cultural and behavioural improvements.

(3) It was important to take a holistic view of mitigations to ensure a consistent and mutually supportive approach to addressing risk.

(4) The risk descriptor would benefit from target dates/milestones and a clear description of desired end-point. Given that of the eleven key mitigations outlined, eight were in need of improvement there was a case for moving overall mitigation effectiveness from “needs to improve” to “critically deficient”.

(5) Given the extreme likelihood of hostile action against the University, there was a strong case for a third party independent cyber risk assessment. In light of the current external environment, the rating of the risk should be moved from “very likely” to “almost certain.”

(6) The next major incident response planning exercise would feature cyber vulnerability as a key element.

ii) Major Regulatory Incident related to Information Security and Data Protection

Noted:

(1) There was some overlap between risk description and mitigations for this risk and the cyber risk.

(2) Risk in this area involved balancing utility with security and there was recognition that there was room for improvement in some mitigations. Excess of personal data and potential consequential enforcement action by the Information Commissioner’s Office was a significant risk.

(3) The importance of building in Information Security and Data Protection measures by design.

(4) There was ongoing gap analysis to address current state and required future state.

iii) Risks related to employee relations

Noted:

(1) As currently described, the risk was primarily externally focused (e.g national position in relation to pay, pensions and the broader industrial relations environment) and there was recognition that it would benefit from the addition of more local context (e.g. impact of transformation programmes) and reference to potential impact on the student experience.

(2) Particularly in the current working environment, the importance of effective engagement and communication in addressing issues relating to staff wellbeing and morale, which should be captured in this descriptor of risk and mitigations. The Board had recently received and discussed the outcomes of the recent Pulse Survey which provided a rich data source in this area. Current activities such as Pulse Surveys and engagement with staff (for example via open meetings) should be captured in the list of mitigations.

(3) An entry error on the three lines of defence measure (which should all be yellow).

iv) Risk of incompatibility between expectations, ambitions and available resources

Noted:

(1) The risk focused on ability to deliver the University's strategic plan in the face of rising expectations and external volatilities with the risk descriptor providing more specific detail.

(2) Effective demand management and clarity about prioritisation were important mitigations, but equally important was cultural and behavioural change to reinforce the above in a period when the University and the sector at large was faced with difficult choices.

(3) Defining and creating a more agile organisation and improving underpinning systems to ensure better and more timely management information to inform decision making were further key mitigations.

(4) The risk description would benefit from the inclusion of key dates and milestones and clearer articulation of financial sustainability constraints and workforce implications.

(5) As currently defined, the risk was too broad and would benefit from review alongside and ultimately integration with Risk 6 (see minute 2 v) below).

(6) There should be focus on ensuring that the articulation of the risk addressed underlying causes and did not just describe symptoms. In this context for both Risks 5 and 6 (minute 2 iv) and 2 v), Root Cause Analysis could be helpful in further refining and integrating these risks.

v) Risk around Sustainable Business/Operating model

Noted:

(1) As noted above, work would be carried out to integrate this risk with Risk 5 (see minute 2 iv above) with the aim of producing a small number of more clearly defined risks.

(2) The risk as currently articulated referenced the financial sustainability issues confronting the sector (including the underfunding of research) and this would form context for discussions on future institutional size and shape and reshaping of Professional Services at the Board Strategy Meeting in July.

(3) In the context of Risks 5 and 6 (minutes 2 iv and 2 v)) it was important to clarify concepts of academic freedom and choice and be clear about the extent and limits of this, given the increased future need to prioritise and direct resource and activity.

vi) Geo-political/over-reliance risks in relation to key countries

Noted:

[redacted]

Redacted – restricted information

The Chair concluded the meeting by welcoming the input from members and confirming that future scheduling would incorporate a rolling cycle of reviews of the most significant risks.

Action: The RSCOO, Director of Compliance and Risk and Deputy Secretary would follow up on comments and suggestions outlined above in development of the next iteration of the risk. Further detailed comment should be sent to the Director of Compliance and Risk.