CONFIDENTIAL

Minutes of the extraordinary meeting of the Group Audit and Risk Committee held at 5.00 pm on Thursday, 28 October 2021 via MS Teams

Present
Duncan Brown (Chair)
John Cole
Mark Lemmon
Rob Orr

Apologies
Richard Flatman

In attendance
David Phoenix
Natalie Ferer
Kerry Johnson
Stuart Johnston
Nicole Louis
James Stevenson

Observer
Kate Stanton-Davies

Internal auditors (BDO)
Nicola Walker
Gemma Wright

1. **Welcome and apologies**

The Chair welcomed members to the meeting.

The above apologies were noted.

2. **Declarations of interest**

No interests were declared on any item on the agenda.

3. **Cyber incident review**

The committee discussed the Executive's review of the December 2020 cyber incident.

An external consultancy had reviewed the method of attack but had not identified the vector or root cause.

The committee noted the actions taken and improvements made to key systems since the cyber incident. Steps had been taken to mitigate key security risks through, for example, network segmentation and new firewalls. In addition, new systems would be appropriately documented.

The committee noted that the network replacement project was funded over the medium term and underway. Project LEAP would also eliminate a number of legacy systems, including the current QL student records system. In addition, multifactor authentication would shortly be introduced to all staff, which was an opportunity to raise awareness and communicate the importance of cyber security.

The committee discussed lessons learned from the incident, which fell into two categories:

1. low IT operational maturity (people, processes and technology); and
2. a technology capability gap (staff skills and capacity).

The committee queried the organisational structure of IT, and the department’s links with other parts of LSBU. The committee noted that the Group Director of IT was responsible for IT service delivery, IT change and innovation, and IT security, and reported directly to the Chief Customer Officer. The committee requested that an organisational chart be circulated to provide clarity on reporting lines.

The committee noted that the University planned to submit its application for Cyber Essentials accreditation before the end of 2021. This would lay the foundation for a further submission for Cyber Essentials Plus in two to three years.

4. **IT disaster recovery internal audit report (draft)**

The committee discussed the LSBU Group IT disaster recovery draft internal audit report. For LSBU, the report provided “no assurance on the control design and a limited level of assurance for the operational effectiveness of the controls in place”.

For SBC the report provided a limited level of assurance for both the control design and the operational effectiveness of the controls. For SBA the report provided a moderate level of assurance for the control design and a limited level of assurance for the operational effectiveness of the controls.

The committee noted that the internal audit made nine recommendations across the Group, four of which were high risk, four medium risk and one low risk.

The committee noted the steps being taken to address the report’s recommendations and mitigate risks, including the network replacement programme, referred to above.

The committee noted that the majority of the work required had already been discussed by the Executive and there was not expected to be a substantial need for additional funding, beyond what had already been budgeted.

The committee noted the focus on developing and upskilling the existing IT team.

The committee noted that a complete disaster recovery plan was expected to be in place by January 2022.

The committee noted that full management responses would be drafted, and would be brought to an additional meeting of the committee in January/February 2022, alongside a fully-costed and achievable action plan to address the report's recommendations. BDO agreed that management needed to take time to respond in full, given the context of IT over the previous year.

5. **Cloud migration: fact finding and lessons learned**

The committee discussed the Executive's detailed fact finding and lessons learned report on LSBU cloud migration.

The committee noted that five internal audits of IT had been carried out between 2013 and 2021. Each audit had a specific focus and covered different aspects of IT, though overall the audits showed that IT governance and security represented a high degree of risk to the organisation.

The committee noted that, at the time of the cyber incident, almost all applications had been hosted on-premises rather than in the cloud. The committee discussed the timeline of decisions made relating to the move from the IBM cloud back to on-premises, noting that this was intended to be a temporary solution prior to the transfer of most applications to a public cloud.

The committee noted that a high level proposal on the migration had been presented to the Executive in 2018 but that the complexity of the work required, timescales and full cost were not sufficiently well communicated.

The committee noted that an IT security and resilience board was now in place, co-chaired by the Chief Customer Officer and Group Secretary, which had oversight of security measures across the Group and would start to scrutinise some IT-related projects. The committee noted that LSBU did not have a PMO function, but that a new approach to oversight of large projects would be proposed to the Executive during November 2021.

The committee requested to review the local IT risk register at a future meeting.

Date of next meeting
5.00 pm, on Thursday, 11 November 2021

Confirmed as a true record

Duncan Brown

.... (Chair)