Minutes of the Audit Committee meeting held on 16 March 2021
online by Teams starting at 6.15 pm

Present	Lucy Lee (Chair) Badri Gargeshnari Geraldine Swanton Harrison Thompson Tony Worth
In Attendance	John Callaghan (Principal) Lindsey Stewart (Deputy Principal and Stratford Chief Operating Officer) Heather Evans (Vice Principal Finance) Pete Haynes (Vice Principal HR and Student Services) Sam Bromwich (Director of Risk, Control and Compliance) Dave Gartside (Director of IT) Theresa Lynch (Clerk) Louise Tweedie (Partner – RSM)

The meeting was recorded.

1. Apologies for Absence

Apologies for absence were received from Paul Large and it was noted that it would have been his final meeting as he was standing down as a Governor on 31st March 2021. Thanks were expressed to him for his contribution to the Audit Committee.

The Chair welcomed Harrison to his first Audit meeting as an External Member and introductions were made, as appropriate.

2. Declarations of Interest in relation to this agenda

No new declarations of interest were received.

3. Minutes of the Audit/Corporation Meeting held on 30 November 2020

The minutes of the meeting held on 30 November 2020 were agreed as a true and accurate record and signed with the Chair's e-signature.

3.1 Matters Arising

There were no matters arising.

3.2 Actions

It was noted that there were two Actions for discussion:

3.2.1 Internal Audit Plan

The Vice Principal Finance noted that in March 2020 the Committee had indicated that the internal audit plan for the following year be considered at the March meeting each year. However, on reflection it was felt that this was too early in the cycle to be able to identify the key risks that would initiate an internal audit. It was necessary for the Corporation to agree the Strategic Plan to be able to identify the key strategic risks. It was noted that the May Corporation meeting had now been redefined as a strategy meeting to consider the draft Strategic Plan and strategic risks in terms of

planning for subsequent years. This, therefore, meant that the June Audit Committee would be appropriate for agreeing the Internal Audit Plan.

The Chair noted that the Action had been identified to respond to the Committee's wish to be more involved in the development of the annual internal audit plan. The Internal Auditor explained that this was happening increasingly across her client base. She noted that she would be able to provide a perception of the external environment and indicate possible options for the plan. The Clerk explained that the May Corporation meeting would be an opportunity to consider strategic planning and risk and that it may be possible to incorporate an Audit Committee session to begin the internal audit planning process too. The Clerk and EMT would scope out the agenda for the evening. **Action**.

3.2.2 Exception-based Reporting

The Director Risk, Control and Compliance outlined issues arising from the implementation of exception-based reporting to address the length of the reports. It was noted that the College was proposing a return to the former reporting approach because the required detail was not available in the report. Discussion took place on the relative merits of both, and it was agreed to revert to the longer, full reports that gave more context, detail and a better representation of the audit, as well as, providing executive summaries for quick reference of issues and recommendation. The Internal Auditor reiterated that exception-based reporting did remove a lot of information that was useful for the Committee to be aware of in terms of the approach to the audit and areas covered that had not raised an issue. The full report provided a more comprehensive picture of the audit work covered.

4. Risk Management and Board Assurance Reports

The Director of Risk, Control and Compliance gave an overall update on the risk management and board assurance reports.

4.1 Current Overarching Strategic Risks

The Director of Risk, Control and Compliance presented the key risks that had been identified through the Compliance, Value for Money and Risk Special Interest Group. The Group had recommended that the Corporation engage with the top risks at each meeting and that the agenda reflect the current issues identified. The report had been re-named to Current Overarching Strategic Risks and was reviewed regularly to review the risks and indicate mitigating Actions being taken. The report would be presented as part of the Strategic Risk Register and Board Assurance Framework report at each Audit Committee so that it could be reviewed alongside the Risk Register. The Director of Risk, Control and Compliance described the key risks and mitigation being taken to manage them. She noted that a 4th key risk had been added relating to re-opening in March 2021.

Q. Clarity was sought in relation to risk 3 – The College's IT systems are compromised due to a cyber-attack – and whether there was any data to indicate the number and levels of attacks and to inform 'likelihood'?
A. The Director of IT explained that last year there were 20 HE and FE institutions that had to close due to a cyber-attack. In relation to the College, specifically, the introduction of the "SIEM" system was likely to produce this kind of information. It is likely to facilitate a traffic-light system of what the College's cyber risk looks like. It was noted that some data on the number of attacks and potential attacks would be useful to ascertain likelihood and the overall potential risk. It was noted that there would be a regular update report on IT for the Corporation that could include this information.

Discussion took place regarding the process for the current overarching strategic risks document in relation to Corporation and the Audit Committee.

The Chair suggested that direction of travel in relation to each risk would be useful to demonstrate relative 'movement' of the key risk for Governors. **Action**.

4.2 Strategic Risk Register and Board Assurance Framework

The Director of Risk, Control and Compliance presented the Strategic Risk register and Board Assurance Framework and explained that it had been reviewed internally by the Risk Management Group. The key risks relating to COVID-19, Apprenticeships and HE were reflected throughout the Register.

It was confirmed that there were currently no reports providing independent board assurance.

4.3 Reset and Recovery COVID-19 Risk Assessment

The Director of Risk, Control and Compliance presented the Reset and Recovery COVID-19 Risk Assessment. All cross-College area risk-assessments had been updated in preparation for the COVID-19 testing programme and for student and staff return in March 2021, in line with Government requirements, as well as specialist guidance for some curriculum areas. The overall Reset and Recovery Risk Assessment had been updated and uploaded to the Governors' Dashboard. There were separate LFD risk assessments for the testing sites that linked into Solihull MBC and Public Health England for both Solihull and Stratford upon Avon campuses.

The Principal noted that there had been only 6 positive tests out of about 3,800 tests across the College. It is likely that after a few weeks of being open and with home testing the rate may increase, but this had been a positive start and did not seem to reflect the assertion that a high number of teenagers were likely to be asymptomatic. It seemed that taking the first week to get the testing underway was a good approach, as a number of colleges are finding that they have had to isolate groups due to higher rates of infection. He thanked the Deputy Principal, the Vice Principal HR and Student Services and their teams for leading on the testing programme at all campuses.

Q. As the testing is consensual, have there been any issues with student compliance with the testing programme?
A. It has been an approximate 50% testing-rate across the campuses, which is similar to the rates being reported by local schools. Some assurance might be found in the fairly large sample size even at a 50% rate. For Stratford specifically, more use of local testing centres was thought to be in evidence, so centralised College results would not show these results, although some students are providing the information voluntarily.

5. IT Update

The Director of IT's presentation summarised the impact of COVID-19 on IT at the College. New laptops had ensured continuity of teaching and learning and connectivity overall and the College had moved markedly over the last 12 months in terms of migration to Microsoft 365, particularly in relation to use of Teams. He noted that careful planning had taken place to avoid the IT infrastructure team being impacted 'as a whole' by COVID-19, with staff members being assigned in 'bubbles' to support each campus.

The Director of IT explained that there had been stability issues with Hive during the COVID-19 crisis and that the contract had been re-negotiated, achieving cost savings. The College would be moving from VDI to a more traditional Windows model, managed with a tool called "InTune" as well as "AppsAnyWhere" software, allowing the College to manage a portfolio of applications and make them more readily-accessible to students and staff. The changes had been reflected in the new IT Strategy that would be going forward to the Corporation for approval. **Action**.

The Director of IT explained that the College was working with Microsoft to focus on security, moving workloads to the Cloud and windows virtual desktop. Microsoft had provided analytical software that would support the College in understanding usage and security and would allow it to move to Microsoft "Azure". The Director of IT cautioned against over-dependency on a single technology so the results from the Microsoft-funded Windows virtual desktop trial were eagerly anticipated and would be reported to the Committee in relation to how that may shape the College's IT strategy. **Action**.

The Director of IT provided an update on security measures in place to respond to the enduring threats from cyber-attacks, particularly given that a local college had had to close due to their IT systems being compromised in a recent attack. The College had implemented systems that allowed the team to monitor, detect and respond to threats and to generally flag whether the system

was being compromised. He outlined a range of developments to improve security, including the implementation of the "SIEM" [Security Information Event Management] service in collaboration with JISC [formerly the Joint Information Systems Committee] in a triaged approach which deposited log-data from the entire IT infrastructure in one place, heightening visibility and giving 24/7 coverage and on-call provision to leadstaff in the event of a security incident. Another JISC-based management service, "EDURoam" would be put into effect from September 2021. The College had signed up with the National Cyber Security Centre to take advantage of their early-warning service and was committed to achieving the "Cyber Essentials+" status by 31 July 2021, building on its existing "Cyber Essentials" certification.

The Director of IT confirmed Actions that had been taken in response to the Review of IT Arrangements audit and on-going work to address security and IT process issues raised.

Q. Do you use permanent fixes or workarounds in place to deal with the authentication of user accounts challenges?
A. Initially, it was a workaround, using HR to authenticate staff's identity prior to resetting their password. However, Microsoft password changing tools using information staff provide as part of the induction process and this is in conjunction with the existing MFA, both of which provide greater levels of assurance.

Q. Could you clarify whether issues related to Hive were on-site ones or remote ones and whether the main challenge was the inability to scale?
A. The issues were on-site ones and the main challenge was the inability of Hive to support the diverse range of applications being accessed by students and staff, so stability has improved since the College reduced the number of applications Hive was expected to deliver.

Q. Did the College receive separate £10k grants from Microsoft per site or just one £10k grant as a whole entity?
A. Microsoft gave a grant to support the process of the Windows virtual desktop 'proof of concept trial', which paid for approximately half of the consultancy costs and half of the Implementation costs with College's Microsoft partner, Phoenix.

Clarity was provided regarding the endpoint detection response that is provided via Sophos.

Q. Is the SIEM service hosted onsite or offsite?
A. The Director of IT confirmed that this was actually both with JISC hosting their own 'splunk' instance in AWS where the data gets ported to and then the College has a number of onsite forwarders on PREM to take the log data and forward that into 'splunk' in AWS.

Q. Does the College have enough bandwidth to support the current heavy usage?
A. Currently, as JISC is in the middle of its "Janet-access programme" the College is doubling up on its Internet links on all three campuses and running them as "active-active", essentially giving two Internet connections in the event of one failing.

Q. How confident are you that the IT Team is receiving the latest information available to enable you to make the right decisions and support you in the work you do?
A. Much collaborative networking has taken place in recent months, so the team is comfortable that is accessing the right level of information. The key issues are to stop depending on campus-specific systems and to recognise the fact that the threat is 24/7 but that staff presence is not, so the strategic aim is to move towards relying on external bodies to provide that 24/7 support. The College is assessing the level and nature of risks continuously and responding with proportionate rigour.

6. Internal Audits

6.1 High Advisory Review of IT Arrangements

The Internal Auditor presented the Review of IT Arrangements audit and noted that RSM Technology Specialist Team had undertaken the review into working arrangements and looking at

2 aspects of the Cyber Essentials Plus framework. Colleges will be expected to achieve this standard by 2022. The auditors reviewed whether there was a documented process in place in response to the framework. It was found that practical processes had been put in place, but not necessarily always documented. She noted that during the pandemic the nature and level of risk had changed markedly. The increased scale of the risk within the education sector was reflected in the number of high and medium priority Actions, as the sector had embedded technology so extensively in response to the increased need for remote working.

It was noted that the challenge was to keep addressing constantly changing and increasing sophisticated threats, whilst understanding that it was not possible to be 100% secure. The reliance on IT was now fundamental for all organisations and so required an on-going focus.

Q. Did RSM extend the test enough or leave it with the ICT Team after it was found that 5 out of 15 leavers still had access after their departure?
A. No the tests were not extended – the issue was left with the team to resolve. RSM would do a follow up audit in 2021/22 that would provide feedback. However, it was suggested that once further investigation, by the Team, had taken place it would be useful for the Committee to understand how many accounts were still open, as a third of the sample was found to be in error. **Action**

Clarity was sought regarding the section relating to the patching processes and the introduction of SIEM tool 'to provide security for the entire estate'. The Internal Auditor confirmed that the two areas had seemed to be conflated and confirmed that SIEM would identify vulnerabilities, but not fix vulnerabilities, as the reports seemed to imply.

Q. Is there going to be a follow-up in relation to this audit?
A. Yes, follow-up normally takes place in the following academic year. However, it may be useful to follow-up the high priority Actions prior to production of the Internal Auditors Annual Report. This would mean that in the summer an internal auditor specialist technology team may follow this up with the IT Team to identify progress.

Q. Do other colleges follow up this kind of audit more often?
A. No, you would not expect to see internal audit following this up more often, but you would expect internal checking processes to be regularly addressing these issues. The sector was increasingly engaging external companies to carry out system-access-attempts to test processes and systems. It was anticipated that IT audits were likely to feature more regularly in the internal audit cycle in the future, but it was key that the IT Team update on progress more regularly.

Q. In the event of a serious ransomware attack what might the response be?
A. Guidance from the National Cyber Security Centre and the AoC is clear about not paying ransom demands. Insurance companies have taken some colleges to court in response to claims made on them to reimburse ransom payments made, on the basis that certain college controls were insufficiently robust and therefore those colleges were liable. Ransomware is ultimately a test of system 'back-ups' and also the timeliness of data recovery especially when it comes to cloud providers.

The Vice Principal Finance reported that a contingency plan was being devised in the event of a cyber-attack and, when appropriate, they would meet with South and City College to discuss lessons learned. Further, the Director of Compliance, Risk and Control would be setting up a mock incident to test the systems and to work through the issues with College Management Team to test effective incident-management planning and processes for each area and to consider the implications of different timescales.

The Director of IT was thanked and he left the meeting.

6.2 Key Financial Controls

The Internal Auditor presented the Key Financial Controls audit and noted that controls relating to remote and blended learning were included and how processes had been amended accordingly. A green level of assurance resulted from this very positive audit with two recommendations arising. One was low priority and the other was a medium Action around supplier amendments and additions. Aside from cyber issues, this was still the biggest area of fraud in the sector with people

being tricked into making amendments that are not genuine, often changing low level details initially and following up with change of bank details. Identity authentication is key in this and requires clear documentation of processes and approval mechanisms.

Q. In relation to the draft reporting process, is it typical that there will be a number of iterations prior to the conclusion?
A. No, it is not typical to go through this number of iterations. In relation to this report, the conclusion did not change, however, there were some amendments relating to context and narrative to ensure a clear message. Sometimes this is more difficult in the exception-style reporting and this does underline the usefulness of having the full report and would probably reduce the number of iterations in reaching the finalised report. It was noted that the virtual audit process and reviewing reports via Teams also possibly added elements to this process.

6.3 Progress Report

The Internal Auditor presented the progress report and confirmed that they were on track with the Internal Audit Plan for 2021/22. There were still 3 reviews to be completed. She thanked the College for responding so well to online audits and remote meetings. It had allowed them to continue providing its reports and completing its work, relying on the College to do much of the evidence gathering until such time as on-site audits could resume.

The Internal Auditor noted that the RSM briefing on risk appetite identified an increasing focus on this in the sector. The ESFA's January 2021 guidance for Academies required them to formally document their risk appetite to guide their board-level decisions and the July 2020 Ney Review recommended that FE audit committees took a key role in advising the board on its risk appetite and suggesting this be built into the Audit Code of Practice. Although this had not yet been incorporated in the Code, it was anticipated that this would happen and, therefore, it would be useful for the College to consider developing their framework. The FE Commissioner's Office had identified this as an element of good strategic and financial oversight and ensuring that decisions are based on a college's documented risk appetite framework.

6.4 Benchmarking Report

The Internal Auditor presented the benchmarking report and noted that it provided an analysis of the levels of assurance and the number and category of Actions on a historic-trend comparison, and was noted to be another positive report for the College.

7. Health and Safety Termly Report

The Vice Principal Finance presented the report and noted that there had been some reviews of area risk-assessments as part of the re-opening of the College. Compared to previous years, accident and incident statistics were understandably low given the closure periods for the College. Staff online training was continually monitored to ensure mandatory courses were completed. One outstanding insurance claim had been closed by the insurers. The College was keen to encourage more staff to train as first-aiders to avoid over-dependency on a core group of staff volunteers and to ensure coverage during continued 'working bubble' arrangements.

Q. How are Display Screen Assessments [DSE] being monitored with staff working more remotely, with a particular focus on any musculoskeletal issues emerging from the variety of home-working environments?
A. Staff bulletins have been issued during lockdown periods with advice and reminders about taking breaks. Anyone unable to work from home has been able to request on-site working. Equipment has been provided on a loan basis where necessary.

8. Value for Money Termly Report and Policy Review

The Vice Principal Finance presented the value for money report and noted that the Policy and a new reporting format had been discussed at the recent Compliance, value for Money and Risk Special Interest Group meeting. Key KPIs on the themes of economy, efficiency, effectiveness - had been identified to enable monitoring annually. The mock report was being presented as an example of the approach with the next step being to produce the report for Corporation on 27th May

2021. The report included a range of activities including procurement, but also captures OfS expectations of value for money, such as, student complaint information, outcomes etc.

The Internal Auditor explained that the OfS tended to monitor value for money in terms of whether the student received value for money in relation to the fees they pay, by looking at outcomes and destinations. They consider value for money for the taxpayer too. By contrast, the FE sector VfM focus was a more traditional one, looking at economy, efficiency, effectiveness, and this approach was also included in the OfS' Value for Money Strategy, published a year ago. She noted that she would share any examples of good practice from her client-base.

The Vice Principal Finance explained that procurement savings were set out in the appendix and noted that it was becoming more difficult to make savings, as the exercise had been undertaken a few times. Competitive quotes were obtained for all items over £5k, to ensure value for money was delivered.

Resolved to recommend approval of the Value for Money Policy to Corporation.

9. Policies for Review

9.1 Business Continuity Policy and Incident Management and Business Continuity Plan

The Director of Compliance, Risk and Control presented the Business Continuity Policy and Incident Management and Business Continuity Plan. The Plan reflected College processes and its approach to incident management and had been updated in line with the impacts of the COVID-19 crisis and cyber security considerations.

Q. Is there a record of 'return-to-operation-times' for some key systems in the event of any serious incident?
A. The College approaches this the other way round by having a Business Impact Plan where an assessment is made of how long the College would 'survive' certain things, so for example, being off-site and then what would be needed to support the service off-site. Timescales are included to some extent, based on specific incidents, and shows how long the College could survive, rather than set a timeframe to work to. The Principal noted that staff might be asked to plan and prepare for one week as a reasonable approach, which in itself would illustrate the difficulties of preparing for any longer period of time and would also need to take account of the wide variety of potential incidents that could impact.

Resolved to recommend approval of the Business Continuity Policy and Incident Management and Business Continuity Plan to Corporation.

9.2 Whistleblowing Policy

The Clerk to the Corporation presented the Whistle-blowing Policy and explained that some minor updates had been made as well as changes to include the Office for Students (OfS) as a body that an employee may wish to report an issue to.

Q. Could you clarify what is meant by 'contractors' in the Policy?
A. The understanding was that it referred to those employed as contractors but who were based on-site, such as cleaning staff. Clarity would be sort regarding inclusion of contractors in the Policy. **Action**.

Resolved to recommend approval of the Whistleblowing Policy to Corporation, subject to clarity regarding 'contractors'.

The Internal Auditor left the meeting for consideration of items 10,11 and 12.

10. Recruitment of Internal and External Auditors [confidential section].

This item was deemed confidential.

11. Notes of the Audit Services Tender Special Interest Group [SiG] had been included for information.

This item was deemed confidential.

12. Review of External Auditors' Performance [confidential]

This item was deemed confidential.

13. All Additional Audit Work

This item was deemed confidential.

14. Notes of the Compliance, Risk and Value for Money Special Interest Group meeting held on 3rd March 2021

The notes of the Compliance, Risk and Value for Money SIG were received for information.

15. Management Report on Implementation of Recommendations

The Director of Risk, Control and Compliance introduced the report which was for information – noting that it tracked all internal audit recommendations, Actions and progress and that the same process was used for the ESF audit. The Vice Principal Finance noted that EMT used the report routinely to ensure that managers were following up on any agreed required Actions. There were also follow-up audits conducted by the Internal Auditors - and the tracker report provided good ongoing preparation for this. It was also noted that Governors' attention would be drawn to any overdue Actions and a narrative provided for any agreed delays or changed implementation dates.

16. Date of the next meeting

The date of the next meeting was scheduled for 6pm on Monday 14 June 2021.

The meeting ended at 8.20pm.

Signed  Date **14 June 2021**

Confidential Minutes of the Audit Committee meeting held on 16 March 2021 online by Teams starting at 6.15 pm

Present	Lucy Lee (Chair) Badri Gargeshnari Geraldine Swanton Harrison Thompson Tony Worth
In Attendance	John Callaghan (Principal) Lindsey Stewart (Deputy Principal and Stratford Chief Operating Officer) Heather Evans (Vice Principal Finance) Pete Haynes (Vice Principal HR and Student Services) Sam Bromwich (Director of Risk, Control and Compliance) Theresa Lynch (Clerk)

The meeting was recorded.

10. Recruitment of Internal and External Auditors [confidential section].

10.1 FSA Auditors – external audit

10.2 Internal Auditors

10.3 Notes of the Audit Services Tender Special Interest Group [SiG] had been included for information.

12. Review of External Auditors' Performance

13. All Additional Audit Work