

AUDIT COMMITTEE MEETING MINUTES

Date: 2 July 24

Venue: Board room

Time: 5.30pm

Chair	Richard Smith Morgan
Corporation Members	Stephen Critoph (online)
Co-opted Members	Thana Nathan
Auditors	Katharine Patel - Auditor (External - Buzzacott) to item 6 Dakshita Takodra – Auditor (Internal Audit – TIAA) to item 8
Officers in attendance	Gerry McDonald: Group Principal & CEO Jamie Stroud: Group Director of Finance
Observer	Rachel Robson: External Board Reviewer
Apologies	All members were present
Minutes	Elsa Wright – Director of Governance

Item No	Item of business
1	Welcome and Introductions The Chair welcomed everyone to the meeting.
2	Apologies for Absence All Members were present from item 8.3. The meeting was not quorate for items 1-8.3.
3	Declaration of Interests None received.
4	Minutes of the Last Meeting held on 29th February 2024 The minutes of the meeting were agreed as drafted.
5	Matters Arising and Action Points from the Meeting The action points were reviewed.
ITEMS FOR DISCUSSION, DECISION OR ACTION	
6	External Audit Strategy The External Auditor, Katharine Patel from Buzzacott, introduced her paper, commenting that the audit and framework were stable and that the paper set out the fee quote. The scope of the audit, which was the same as the previous year, was outlined on page 3.

Item No	Item of business
	<p>The audit was similar to the previous year with very little change to the Code of practice. The papers set out the fees and the scope on page 3. Two of the subsidiaries had been struck off with just the Oxford School of English to be audited separately.</p> <p>Page 4 showed the key timetable and dates. There would be a report back to the Audit Committee in early December. Pages 5 and 6 showed the financial statements audit and regularity assurance plan. The new Financial Handbook was applicable from 1 August 2024.</p> <p>The table starting on page 7 showed issues of audit significance identified in the pre-audit planning which needed to be followed up. The going concern assessment and financial position was looking positive with a surplus forecast. Pay costs and utilities had increased. After the merger with BSix, their results would be brought into NCC plans.</p> <p>Page 8 of the report covered income side. The audit would follow the usual pattern with an assessment of risk, including apprenticeships and accuracy of the ILR. 16-18 funding was lagged so there was less risk from an income recognition basis. There were a number of significant capital projects with three listed in the report. There was a risk around trying to capitalise more costs including feasibility costs for a capital project. The audit would look at the costs being carried, such as professional fees, to see if they are valid or whether they should be written off in year. This would look at questions such as, are they adding value to the asset. The normal rule was that feasibility costs were for assessing an option and that once planning was secured, costs incurred could be capitalised.</p> <p>Governors asked whether this was something that had been reviewed before or if this was a change in position. The auditor explained that it would have been reviewed as part of the audit but the sums were more material this year. There had been nothing to write off previously on other projects. NCC might want to write some off costs now rather than capitalise them. There may also be some costs for Ardleigh Green which was a live project. It was agreed that the auditors could look at evidence post year end to see whether any conditions had been met.</p> <p>Page 10 of the report covered regularity and would include the Managing Public Money requirements. It was noted that there had been an incident where a supplier had been paid twice. The Finance Director explained that it was a clerical error and not material at £59k. There was an action point for the FD to revert on progress in relation to the ongoing legal action. The CEO commented that a conversation about write offs with the Finance Director would be helpful.</p> <p>Management override of controls would be reviewed and this would include looking at the use of journals. One area of focus was the OSE and it was noted that systems were much more robust as it had been brought onto NCC systems. It was not material, but a report was needed as a subsidiary.</p> <p>Page 11 covered related parties, accounting estimates and inherent audit risks.</p>

Item No	Item of business
	<p>The auditor reminded the committee about the importance of mitigating the risk of fraud. There was nothing to suggest that there was anything but it would need to be reported if found. The fees were set out on page 13. Appendices 1 and 2 covered the changes to the Accounts direction and the audit code as well as the terms of engagement which were in line with the previous year.</p> <p>It was noted that the fee for OSE seemed relatively high as it was now in a different place to the first audit last year. It was agreed that this would be looked at during the planning day.</p> <p>The auditor asked whether the plan was still to merge the OSE. There were some issues to resolve and the move last year to incorporate the other subsidiaries was in relation to the changes to loss making subsidiaries which needed a DFE letter if support under the MPM guidelines. It was noted that the controls were not sufficient when NCC acquired the school and that they were very different now.</p> <p>It was confirmed that the audit fees in the budget. The committee thanked the external auditor for her report and she left the meeting.</p> <p>ACTION – Fee for OSE audit to be reviewed at audit planning day – Group Finance Director to follow up</p> <p>ACTION – the committee noted the external audit plan. The report would be included in the Board reference pack for all Board members</p>
8	<p>Internal Audit Service (taken as item 7)</p> <p>8.1 Internal audit reports</p> <p>There were three reports presented to the meeting for discussion. Safeguarding had received substantial assurance with one recommendation which had been discussed at the March meeting.</p> <p>Health and Safety had received reasonable assurance with two recommendations around policy and sample inspections. There were some minor risks around updating policies and risks assessments. The culture, awareness and ownership of health and safety was good.</p> <p>Accounts payable and general ledger had received substantial assurance with 2 minor recommendations on signing off reconciliations.</p> <p>There was a discussion about the Health and Safety actions with some of the recommendations being very operational and in line with the previous audit. The internal auditor explained that most had been passed and then they would be reviewed and go on the tracker to be verified and reported as closed.</p>

Item No	Item of business
	<p>There were three further audits on the 2023-24 plan which were in progress and would be reported to the first committee in the autumn term.</p> <p>Governors asked about the Health and Safety audit and whether there were any items that were a cause for concern. The internal auditor explained that this was in line with expectation and that this was an additional report to look at some other campuses to check that what was seen elsewhere was in line across the group. Overall culture was good and that was key. Most recommendations were low level and operational. There was a discussion about whether the audit should be more frequent than every three years. Information about how quickly the issues were dealt with and cleared would help with this discussion. The internal auditor confirmed that this would be reviewed as part of the audit universe at the next meeting which would conclude the 2023-24 programme.</p> <p>ACTION – frequency of Health and Safety audits to be reviewed as part of the audit universe discussion at the October meeting</p> <p>8.2 Progress on implementation of audit recommendations</p> <p>The internal auditor would merge this report with the follow up that they conducted and this would be reported back to the October meeting. Almost all of the recommendations had been implemented and this would be verified before final sign off.</p> <p>ACTION – report for October committee from TIAA on implementation of audit recommendations</p> <p>8.3 Audit Strategy and Plan for 2024-25</p> <p>There had been some comments around the governance audit and performance management and the internal auditor confirmed that she could send some further information and the updated plan for review before it was finalised. The CEO said that the definition of performance management was key. It was noted that there had been discussions about auditing further sites to look at Health and Safety but this was not in the current plan.</p> <p>Thana Nathan arrived.</p> <p>It was agreed that an offline discussion was needed before the plan was firmed up. The Chair would review the plan before it was recommended to the Board for approval.</p> <p>The internal auditor left the meeting.</p> <p>The role and remit of the audits were discussed. It was key that they added value. The view was that they needed to be more strategic and both value added and quality were needed from the service.</p> <p>ACTION – offline discussion to take place before plan finalised for the Board</p>

Item No	Item of business
7	<p data-bbox="233 327 778 365">Managing Cyber Risk (taken as item 8)</p> <p data-bbox="233 409 1469 600">The Group Director IT joined the meeting and explained that cyber security was an ongoing risk which was taken seriously as part of the management of the network. It was under constant review and she hoped that the presentation would offer governors reassurance about the efforts that were being taken to maintain the integrity of the system.</p> <p data-bbox="233 645 1442 835">The college had been audited by JISC and was seen to be one of the best in the sector. JISC ran the JANET networks which were used by academic institutions including colleges and universities. There was an annual report each year. The Board had been briefed in the cyber security live exercise which took place last year to take down all the college systems.</p> <p data-bbox="233 880 1469 1144">Governors were keen to understand what kept her awake at night and that they should be concerned about. The biggest threat was to education and college were high risk due to the amount of data they held. Colleges were targets for credential harvesting which included malware, phishing, and social engineering. There were also attacks using ransomware, data theft and data loss. Data loss could relate to any data held. Finance was on a remote access system. Two factor identification was in place across the college for both staff and students.</p> <p data-bbox="233 1189 1469 1339">The cyber threat to NCC could have an impact on teaching and learning and business operations and there could be significant costs of recovery and reputational damage. It could cost £2m to recover from an attack and there could be further financial implication through the loss of contracts.</p> <p data-bbox="233 1384 1449 1534">The presentation set out a list of systems and processes which were used to protect the networks. These included firewalls and web filters, anti virus and malware protection; endpoint protection which looked at bigger pictures and behaviour. The system passwords could not be saved as a preventative measure.</p> <p data-bbox="233 1579 1461 1769">Privileged identity management applied to all IT system access with engineers having to seek permission from peers and senior managers to access systems and make changes. Systems were separate for staff and students. Techniques such as system hardening to remove unwanted software and patching were in place. Back ups were created every night.</p> <p data-bbox="233 1814 1449 2004">Senior systems engineers conducted live monitoring and there were 25 staff in the team with a few key staff. JISC services monitored all logs 24/7. They were tracked and read automatically. Cyber security threat management was in place which could pick up concerns before staff on the ground could see issues. This offered a high level of assurance.</p>

Item No	Item of business
	<p>Audit of systems was good with JISC monitoring covering denial of service attack detection and Domain name service filtering. They also provided threat intelligence and account protection.</p> <p>JISC provided the NCC internet connection via the JANET network. This was a university standard connection that cost £83k per year and included Ebooks and library access. This offered very good value for money and gave the college huge capacity for connectivity</p> <p>The Group Director outlined how the systems were checked. Audits were completed by the college’s insurers and by JISC. The college was Cyber essentials/plus accredited. Vulnerability assessment and penetration testing were completed both externally and internally alongside a monthly network scan. JISC had tried twice to get into the system. There had been a review and some remedial work which included systems and process changes. Advice was taken from the national cyber security centre on best practice. System access codes were stored in an online vault. They were generated randomly and access was logged and two step.</p> <p>The aim was not the make impenetrable but to make it hard so that those trying to gain access would go elsewhere. It was important to ensure that the college was doing everything it could. There was both online and face to face training for staff. The scenario-based attack in 2023 had been planned with only five people aware that it would happen. It was a real time attack and all systems had to be brought back online. This had led to some improvements and learning for all involved including the IT team.</p> <p>The Board noted that the current BSix system was cloud based but they would be using the same system as NCC following merger. It was anticipated that email migration and timing would be the most difficult part. Staff would need to get used to a different level of security and filtering with internal firewalls and MFA.</p> <p>Phishing was an area of concern and staff did fail the test. Those who had opened two messages had been given face to face training. There would be an HR process for repeat offenders and this had been communicated to staff. They were aware that they would not get a second chance elsewhere. There were repercussions if access was blocked such as registers not being taken which was key. Some staff were not opening messages which was difficult. There was a balance between security and access.</p> <p>Governors asked about the value of JISC audits. They were incredibly valuable and would tell the college where changes needed to be made. They chose what to audit, and it was good to have an external view. Internal audits tended to focus on paperwork rather than systems.</p> <p>Governors thanked the Group Director her report which was very helpful and offered assurance of the systems in place to keep the college safe.</p>

Item No	Item of business
	It was confirmed that JISC were an independent organisation. A lot of the reporting was very technical but summaries could be provided for the committee when testing took place.
9	<p>Risk Register and Risk Policy</p> <p>9.1 Risk Policy</p> <p>Following agreement at the autumn meeting, the Chair of the Committee and the Deputy CEO had been tasked with working on the College’s risk policy, to include a review of the Board’s Risk Register format and risk appetite. The CEO had taken on this work with the Chair of the Audit Committee and presented a proposed risk management policy, which consolidated existing practices, and asked for comments. The draft risk appetite statement included indicative time frames. This was the first articulation of risk appetite and comments would be welcome from Board members at the Corporation meeting.</p> <p>Following discussion, the Committee AGREED to recommend the draft documents to the Board for approval.</p> <p>ACTION – the committee recommended the risk management policy for approval by the Board</p> <p>9.2 Committee Monitoring of Risk</p> <p>The Committee were reminded that they were tasked with monitoring the item under Quality and financial viability of apprenticeships relating to distance learning data management. Following discussion, the Committee were satisfied that this was now closed and could be removed from the risk register. The Committee received the feedback on risk management monitoring from each of the other Committees. The monitoring of the risks was covered in regular reporting to each committee.</p> <p>Action – Distance learning to be removed from the risk register</p>
10	<p>Attempted Fraud</p> <p>The Committee noted that there had been no fraud attempts since the last report. There were no irregularities or improprieties to report.</p>
11	<p>Any Other Business</p> <p>There were no items of any other business.</p>
12	<p>Date of Next Meeting</p> <p>Provisional date – Thursday 10 October 2024 – to be confirmed at the Board on 11 July 2024</p>

The meeting closed at 6.50 pm