



# THE CORPORATION OF THE SIXTH FORM COLLEGE, COLCHESTER

## Minutes of the Audit Committee Meeting No 70

08 March 2023

[Virtual Meeting held via Microsoft Teams]

**Members present:** S Codling (Chair), M Sherer, J Owens, C Goldsworthy, A Beatty

**In attendance:** I. Fraser, Assistant Principal, N. Goldsmith, Finance Manager,  
G. Rayner, Assistant Principal

**Clerk:** T. Johnson

### 70.1 Apologies for absence

Apologies were received and accepted from E Calderbank

C Goldsworthy had previously given notice that he would need to leave the meeting after item 70.10 Risk Management.

### 70.2 Any other business

70.2.1 It was agreed that the date of the next meeting should be brought forward to accommodate the availability of a committee member.

Date of the next meeting - 15 May, 2023 commencing at 11am.

*Action: Clerk*

70.2.2 Government Digital Accessibility Audit: at the request of the Chair, the Committee agreed to add to the agenda, a report from the College on the findings of the Audit and the actions planned in response. Members agreed that the Committee should receive a report and that it should be added to this meeting's agenda.

### 70.3 Declarations of interest

No declarations reported from the register and none were declared at the meeting.

### 70.4 Determination of confidential items

None identified

### 70.5 Minutes of meeting No. 69 - 22 November 2022

The draft minutes of meeting No. 69 were agreed as a true record of the meeting.

The notes from the working group meeting held 22 November, 2022 were noted. No corrections were requested.

### 70.6 Matters arising

There were no matters arising from the minutes and no pre-meeting questions that had not been covered by the agenda.

### 70.7 Policies, procedures and annual reports

Approval of the following policies was deferred to the next meeting;

- Gifts and Hospitality (cyclic review)

- Treasury Management (cyclic review)

At this point, the Committee agreed a revision to the running order of the agenda.

## **70.8 Consideration of internal audit needs [agenda item 70.11]**

The Chair, drawing attention to the internal audit benchmarking data, asked members for comment regarding any areas where it would be valuable to gain additional assurance.

- 70.8.1 **Cyber Security:** Members identified Cyber Security as a significant area of risk. It was agreed that, subsequent to receiving an update from the Assistant Principal (Risk) on the JISC audit and, after the summer testing of the disaster recovery plans and cyber business continuity work, the Committee would consider whether there were any cyber areas not covered by the external audits and testing, that would benefit from internal audit scrutiny. In the context of new IT systems due to be implemented by the College, the Committee agreed that this matter should be discussed again at the May meeting.

**Action: Clerk**

- 70.8.2 **Procurement, tendering and value for money procedures and assurance:** the Chair highlighted that, whilst this may not be an area for an internal audit at this point, the Committee would like to obtain a greater understanding of the procurement, tendering and value for money procedures undertaken by management. For example, the processes deployed to ensure the correct procedures are being followed and adhered to - it was agreed that this would be an agenda item for the May meeting. Members discussed the general risks associated with tendering and the potential for a single large order to be broken down into smaller orders to negate the need to follow the tendering procedures.

**Action: Clerk/Assistant Principal**

- 70.8.3 **Finance systems:** the Finance Manager reported on the work being undertaken to identify a replacement finance system package and the tendering procedures to be undertaken. It is anticipated that from early 2024, the College will be in a position to test a new system, including running a dual system (old and new systems running simultaneously), with the aim of mitigating the potential risks associated with implementing a new system. It is anticipated that the new system will be fully operational from August 2024.

In response to a member's question regarding value for money, the Finance Manager confirmed that while cost is a driver, the investigative processes being undertaken are with a view to securing the most effective, efficient and future proof system for the College. It is anticipated that the new finance system package will be under the £50k threshold for requiring Board approval.

In the context that changing the finance system is a fundamental decision with associated risk, the Chair asked for a report outlining the rationale for the replacement process, procedures undertaken, and identified costs to be brought to the committee, for information and discussion at the appropriate time.

**Action: Finance Manager/Clerk**

*11.18 Assistant Principal, G.Rayner joined the meeting*

## 70.9 Fraud

The Assistant Principal (External Examinations and Risk), introduced the annual counter fraud reports.

### 70.9.1 Annual fraud risk review – see *risk assessments below*

### 70.9.2 Implementation of the Anti-Fraud, Cybercrime, Theft, Corruption, & Bribery policy and fraud log

The Assistant Principal reported that the fraud log provided assurance to the Committee that the College had zero observed, investigated or reported fraud.

### 70.9.3 Counter-fraud action plan

The Assistant Principal introduced the spring 2023 counter fraud action plan review. Members noted that the actions required to meet the priorities established by the Corporation encompass the elements of counter fraud (prevention, detection, investigation, recovery and sanction) and are driven by the College's priorities and values.

According to the action plan, 19 actions were to be performed during the 2022-2023 academic year. Members noted that 12 actions had been fully implemented within or ahead of the assigned deadlines. 4 actions are in progress, and 3 actions are outstanding. The Assistant Principal, referring to the RAG-rated report, highlighted the actions completed and provided a narrative for those that had not yet been fully achieved. The Assistant Principal explained the reasons why the resources available to implement the action points had been limited and variable.

- i) **Policies and procedures:** all staff have access to all policies on SharePoint. The Assistant Principal will be signposting staff to the Anti-fraud, Corruption, Cybercrime, Theft and Bribery policy with mention in the staff bulletin and associated training made available.

**Action: College**

- ii) **Reporting by members of the public:** a reporting route for members of the public to report suspicions is currently being discussed by management to ensure the most appropriate mechanism is put in place.

**Action: College**

- iii) **Reports to the audit committee:** it is anticipated that in the future, assurance reports received by the Committee will include information on the random sampling of internal controls.

**Action: College**

- iv) **Risk assessments:** fraud risk assessments, including activity undertaken to try and detect fraud in high risk areas where little or nothing is known of fraud levels, will be prepared. At present, the staffing resources have not been available to undertake this section of the action plan.

**Action: Clerk/College**

- v) **Staff training:** the Assistant Principal reported that while the Action Plan refers to 'all staff' training, the College does not have the resources to train all members of staff in a matter, in which many are not involved. As and when training becomes available, e.g. via the SFCA, the priority will be for senior management teams, including the Risk Committee and the finance department staff, to receive training, which will subsequently be cascaded down through the staffing structure.

A member asked how many staff will be trained and what proportion of the whole staffing this represents, and what would happen if a junior member of staff suspected wrongdoing but had not received training on the correct procedures to follow, or is the college view that the obligation under the whistleblowing policy to report such to a head of department covers this?

In response the Assistant Principal highlighted that the Whistleblowing policy covers internal and external reporting, and training isn't necessary prior to anyone making a case. The risk assessment will identify which departments, budget holders, and individual staff with procurement responsibilities, will be required to receive periodic training.

The Clerk highlighted a prior report on staff training covering the 2021-2022 year.

In response to a member's question regarding the timeframes for implementation of training. The Assistant Principal provided assurance that as soon as the risk assessments are completed, an assessment of training needs will be undertaken. The Chair highlighted the need for the risk assessments to be undertaken as soon as possible, with the aim of ensuring training is identified and completed in a reasonable timeframe whilst also acknowledging that proportionality is a key consideration.

**Action: College**

- vi) Ensure all Corporation Members have access to fraud awareness training: the Clerk reported that all Members have access to online training through the ETF both at a basic and comprehensive level. However, according to the self-recorded attendance records take-up has been lower than expected. The Clerk will raise this with the Corporation Chair, ahead of the Chairs' 1 to 1 annual governor development conversations.

**Action: Clerk/Chairs**

The Assistant Principal indicated that the strategy timeframe of July 2023 for the completion or implementation of actions, including management level counter fraud training and the presentation of risk assessments to the Committee, was attainable. However, any general staff counter fraud awareness training would likely be delivered in September, ahead of the new academic year.

The Chair asked the College to provide, for the next meeting, an outline plan of the cyclic and unpredictability counter fraud testing that will take place during the course of a year. The plan will further inform the committee's discussions around internal audit.

**Action: College**

#### 70.9.4 Fraud and Whistle Blowing Cases

The Clerk confirmed that the strategy required a report on Whistleblowing cases and a report on the implementation and impact of the Whistleblowing policy and procedures to be presented. In response to a member question, the Clerk advised the Committee on its responsibilities for overseeing the investigation of all allegations and instances of fraud and irregularity and that allegations of fraud and/or investigation outcomes should be reported to the Committee as soon as practically possible.

The Assistant Principal emphasised that all whistleblowing cases are recorded on the Fraud Log. In this context, members were reminded that the fraud log provided assurance to the Committee that the College had not observed, investigated, or received any whistleblowing reports. The title of the Fraud Log will be expanded to cover whistleblowing.

**Action: College**

## 70.10 Risk Management 2022 - 2023 and Board Assurance

The Assistant Principal (External Examinations and Risk), Risk Register (RR) and Board Assurance Map (BAM)

### Board Assurance Map

The Assistant Principal introduced the update to the Indicative Board Assurance Map (BAM) for 2022 to 2023 (incorporating action plan).

- 70.10.1 **Martyn's Law:** the Assistant Principal reported on a Martyn's Law webinar attended immediately before the meeting and the expectations placed on large premises, including educational institutions. The College is fully committed to ensuring its preparedness for a terrorist attack and is compliant with Martyn's Law 'expectations. There will be periodic inspections that will likely need to be funded by the College. Members recognised the work currently undertaken to raise awareness and maintain a secure site for the safety of the College's students, staff and wider college community. The Assistant Principal advised that should an additional layer of requirements become mandatory, the College may need, in part, to change its ethos.

In response to a member's question, the Assistant Principal outlined the current site security measures and measures taken to empower staff to challenge persons not showing the appropriate identification while on site.

The Assistant Principal provided a verbal update on the significant and seven contingency risks (arising from scrutiny of the risk register and associated information).

- 70.10.2 **Significant Risk: Cyber Security.**

The Assistant Principal provided an overview of the process that has been undertaken following the receipt by management of the JISC audit report. The report praised the IT department, in particular the deployment of multi-factor authentication. The report had made 250 technical recommendations, some of which were either very minor or had already been planned for implementation as part of the Cyber Essentials re-accreditation. The IT team is in the process of prioritising the recommendations, which will inform a cybersecurity action plan.

In response to a question from a member, the Assistant Principal explained why the IT systems technician post remained vacant and the considerations being given to advertising for a more specialist post. The response to the action plan will identify how urgent the staffing needs are.

In this context, the Assistant Principal stressed that while the department would like to significantly increase its staffing resources and respond to the majority of the report, the College will be undertaking as much as it can with the resources it has.

In order to better understand the outcomes of the audit and the levels of resourcing required. Members requested that a high-level summary of the JISC report and the management response, including the level of resourcing required, be provided at the next meeting.

**Action: College**

In response to a member's query regarding benchmarking against other institutions?

The Assistant Principal explained that there is nothing specific in the report.

The Chair asked the College to ascertain whether there is any sector benchmarking and contact JISC to ascertain whether they have benchmarking information.

**Action: College**

A **member asked** whether the findings are rated in terms of severity or urgency, thereby identifying an order for mitigating actions.

The Assistant Principal responded by informing the meeting that the report identifies the 'Top 12' risks. However, on scrutiny of the report, the College's IT team identified that elsewhere within the report there were more significant and higher priority actions (not in the 'top 12').

The **Committee asked** the College to provide insight into the processes for managing the actions and monitoring the action plan, and how management will hold themselves to account for the actions being implemented.

The Assistant Principal explained that the JISC executive summary and the RAG report from the IT team, identifying the department's priorities, will first be considered alongside a management risk/cost/benefit analysis.

In response to a member question regarding the logging and reporting of the number of averted and successful cyber hacks, the Assistant Principal highlighted the significant number that occur daily and the difficulty with reporting all attempts. Members asked for a high level summary to be included with future counter fraud reports.

**Action: College**

11.59 C Goldsworthy left the meeting

In the context that cybersecurity is the biggest risk on the BAM, that cannot be mitigated to a tolerable level, the Committee, as part of the assurance that management are managing the overall risk, wished to obtain a better understanding of the rationale for implementing or not implementing a JISC recommendation. The Chair suggested and members agreed that visibility of the management response plan, an overview of how it is being monitored, ownership of actions and subsequently periodic updates would help members understanding the purposes of an action taken against the risk level.

It was agreed that an executive summary of the JISC report and management response plan would be brought to the next meeting.

**Action: College**

70.10.3 **Disaster Recovery:** a **member queried** how data stored on the Cloud is backed up and what would happen if there were to be an attack on the cloud.

The Assistant Principal referring to the ILT management plan, clarified the situation by providing an overview of the College's internal servers and cloud management. The plans and options discussed by the Board will be finalised before being brought to a future meeting.

Referring to the discussion at the last meeting, members were assured that the Cyber Business Continuity Plan (BCP) testing will be undertaken by JISC towards the end of the year.

**Members asked** whether JISC prepares Business Recovery/Continuity Plans in addition to undertaking testing. The Assistant Principal informed members that management are confident the College has the skills and resources to produce the required plans in-house.

A **member asked** whether the Cyber Essentials accreditation had been received. The submission will be made shortly, and the College is confident of passing.

70.10.4 **Contingent Risks:** members considered the updates to the contingency risks that had not been discussed under item 70.8

A **member queried**, in the context of the recent recruitment difficulties, how the college ensures high quality teaching, where a teacher is required to teach a second subject that may not be their specialism. The Assistant Principal reminded the Committee of the quality assurance processes and assured members that no teacher is asked to teach a subject that they are not happy and qualified to teach and that quality of teaching is not an issue. It was noted that in the majority of cases, the second subject is closely aligned to the first e.g. maths and statistics.

Members agreed that the contingent risks were, as far as possible, mitigated to an acceptable level.

#### **70.11 Consideration of audit needs [see minute 70.8]**

Identification of cross-college areas for the 2022 - 2023 or 2023 - 2024 years

Members considered the Auditor's prior comments regarding the benefits of external scrutiny on particular areas. Members agreed that there were no immediate priorities that required audit at this time; however, this would be kept under review.

#### **70.12 Schedules of committee business**

Members considered the schedules of committee business. No additional items were identified, and members were confident that the 3 meetings a year, with adhoc meetings if required, covered their requirements.

---

### **PART B CONFIDENTIAL MATTERS**

---

#### **70.13 Minutes of the previous meeting**

The confidential minutes of meeting No. 69 held on 22 November 2022, were approved as a true record of the meeting.

Members noted the verbal report on actions taken and discussed the outstanding actions.

#### **70.14 Benchmarking of Auditor Fees**

The Clerk reported on the process undertaken to prepare the benchmarking reports. The Clerk confirmed that the reports only included information from institutions designated as sixth form colleges at the time of the publication of their annual report. The benchmarking reports provided information on fees expended by size of college (funding allocation), region and audit firm.

Following a verbal summary by the Chair and Clerk, Members agreed that the expenditure of the Corporation on its external (regularity, financial statements and teachers' pension) audits was reasonable for a large college with non-complex funding streams. For future years' benchmarking the Committee asked the Clerk to provide in addition to the data a benchmarking summary report.

***Action: Clerk***

It was noted that benchmarking internal audit fees was significantly more difficult, as the precise nature of the work undertaken, any underlying issues and the construction of the

days worked (single piece of work or several engagements) were unknown. However, the data presented was a useful indicator of whether the Corporation was an outlier in terms of not engaging internal audit.

#### **70.15 Review of auditor performance**

The Clerk reported on the review process.

The Corporation's policy for the Review and Retendering of Auditors, requires the Committee to carry out an annual review of the auditor's performance.

To undertake this duty, the Committee obtains views on the performance of the auditor through the provision of written responses to key questions. In respect of the prior year (the 2021- 2022 audit), responses had been obtained from the Finance Manager, Auditor, Chair and Vice Chair of the Audit Committee, and Clerk. Committee Members had also provided responses to a series of key survey style questions, with an option to provide additional commentary where required.

Members noted the query over the timing of the onsite audit work and the auditor's access to the right personnel, and this will be discussed with the Finance Manager.

Having considered and discussed the summary report provided, members agreed that the performance of the auditor had been very good. No concerns were raised.

#### **70.16 Appointment of auditor**

The unanimous decision of the Committee was to recommend to the Corporation the appointment of Scrutton Bland as the external auditor for the 2022- 2023 year

#### **70.17 Any Other Business**

**Government Digital Accessibility Audit:** [see minute 70.2.2]. This will be discussed with the Corporation Chairs and as appropriate, added to the next Corporation or audit committee agenda.

See confidential minutes 70.17

**Meeting Survey:** The Chair reminded those present that the meeting survey provided an opportunity to provide feedback on the meeting.

The Chair of the Committee closed the meeting at 13.05

---

*These minutes were confirmed as a true record on 15.05.2023 Minute No.71.4*

---