Minutes of the Audit Committee meeting held on 14 March 2022, online by Teams
starting at 5.30pm

Present	Lucy Lee (Chair)
	Lindsey Stewart (Acting Principal)
	Geraldine Swanton
	Sarah Horton-Walsh
	Amirun Nehar (External Member)
In Attendance	Heather Evans (Vice Principal Finance)
	Pete Haynes (Vice Principal HR and Student Services)
	Sam Bromwich (Director Control & Compliance)
	Dave Gartside (Director of IT) – for Items 5 and 6.2
	Theresa Lynch (Clerk)
	Louise Tweedie (RSM)
	Mark Dawson (KPMG)

The meeting was recorded.

1. Apologies for Absence

Apologies for absence were received from Badri Gargeshnari and Tony Worth.

2. Declarations of Interest in relation to this agenda

There were no new declarations of interest.

3. Minutes of the Audit/Corporation Meeting held on 30 November 2021

The minutes of the meeting held on 30 November 2021 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 – the actions list was received.

3.3 Presentation Plan to the Audit Committee during 2022/23 - the Chair explained the planned presentations for Audit Committee during 2022/23, to ensure that members receive updates on current key issues for consideration of risks in a more rounded way, to increase involvement in decisions taken on future projects – and to ensure that College maximises the input from internal and external auditors. The presentations were as follows:

- **Cyber Security** – on the current agenda, March 2022
- **Key projects and external funding [with potential clawback]** – June 2022 Audit Committee
- **Sector update from KPMG** – June 2022 Audit Committee
- **Apprenticeships**
- **Deep presentation & discussion on other risks eg subcontractors**
- **Skills Bill [due for release March 2022] & associated risks**

4. Cyber Security Board Assurance Presentation

The Director of IT gave an overview of cyber security, including some of the projects planned along with potential challenges. Badri Gargeshnari had reviewed the presentation and had asked the

Director of IT to highlight the top five risks and mitigations in place. An outline of the recent "phising" exercise implemented by the ICT team was also given.

The Chair thanked the Director of IT for his comprehensive presentation and invited questions:

How do you prioritise, given the complexities outlined so clearly in the presentation with the constant monitoring and assessment of risks in the context of the resources and capacity available in the College?

The approach is to take the highest risk first – and taking account of what the team can action soonest to minimise the risk of being compromised. Some of the risks require significant investment to mitigate, such as the Managed Threat Response, where Governors approved the cost commitment. Other risks are no-cost, the multi-factor-authentication [MFA] being an example, along with the need to maintain staff training. The "24/7-nature" of the threat, set against the "9.00-5.00" team presence was again stressed – highlighting the need to implement the Managed Threat Response.

Q. How do you reconcile the need for security with "ease of access" for those that are less comfortable with ICT?
A. This is a constant challenge and why it is felt a better approach to refocus the ICT team to support end-users in gaining access to systems, which of necessity is becoming increasingly complex. The team is better utilised in this way than being asked to analyse and mitigate complex cyber threats.

Q. In the recent College "phising" exercise can you explain the "tell-tale" sign, within the email, that suggests that it is not a bona-fide email?
A. The firm guidance is not to click on any unexpected email. In the specific "phising" email example shown in the presentation, the email address given is from "Digital Share" and the specific address clearly displayed is "customer_relations@hondaphil.com". It is fully recognised that staff are keen to just do their jobs, are not cyber experts and are simply responding to "easy traps" – something that hackers exploit.

Q. MS Teams – what has been the biggest impact of the college moving to Teams?
A. As the greater use of Teams for documents, folders, meetings and phone calls became established, this exposed the weakness of VDI and as Teams doesn't work on VDI, this meant a return to a traditional model.

Q. Do you feel that the staffing and resourcing of the ICT team is currently adequate, or will it need to be revisited in the future, given the changing nature of the IT environment?
A. Implementing the plan of having a sound Managed Threat Response in place while refocusing the ICT Team on user-support / access-support, is felt to be the right mix. To have an internal Managed Threat Response service and the level of upskilling required for Team staff to meet constantly evolving cyber threats would be too big a proposition, requiring too much in the way of resources.

5.1. Strategic Risk Register and Board Assurance Framework 2021-2022, Review of Top Key Risks and Independent Board Assurance

The Director of Risk, Compliance & Control introduced the top key risks that are part of the Strategic Risk Register, and presented to each Corporation meeting – to clarify their purpose. The risks were noted to be those current at the time of any meeting or discussion, so not set in terms of their number or focus. The eight Area Strategic Risks are the high-level ones, outlined in detail and with clearly identified mitigations, on the Strategic Risk Register, and regularly reviewed. It was noted that the following changes had been made to the top key risks:

- **Added: "The impact of Covid on student achievement and mental health"** - the existing risks associated with Covid had evolved and there was a new focus of mapping its impact on various aspects of learners' experiences and noting any variations among learners since the removal of restrictions on everyone.
- **Added: Appointment of the new Principal**.

- **Remove: "Finance risk"** – this would be retained in detail on the Strategic Risk Register.
- **Remove: "Covid and the delivery of teaching & learning"** – the newer focus on impact, detailed above, suggests that this can move down the list of top risks.

The proposed changes to the list of top risks were **agreed**.

5.2. Risk Appetite / Tolerance update

The Director of Risk, Compliance & Control explained that risk appetite / tolerance would be considered at a Governors' Development session. A questionnaire had been circulated to all Governors to feed in their views.

Q. Do you undertake "horizon-scanning" in the college to identify potential risks in the next six to eighteen months, and if not, whether a one-page summary of medium to longer term risks would be worth compiling to help with planning
A. We have a number of processes in place that undoubtedly fulfil such a role, but we don't specifically approach it using that terminology. The one-page summary is a helpful suggestion that we can look at further and develop. It was noted that KPMG had presented a horizon-scanning exercise at a previous Governors' Development morning.

6. Internal Audit

6.1 Framework for Compliance with Legal Requirements: Data Protection

The Internal audit presented the report and explained that it had been considered timely to revisit data protection since the last audit was undertaken in early 2018 just prior to the GDPR requirements coming into force. Specific focus was given to maintenance of personal data records, arrangements with third parties who have access to College data, retention, training and awareness and the management of data breaches. Only five advisory actions emerged from the audit which are detailed in the report, but overall the audit confirmed that the expected key framework was in place and functioning.

6.2 IT Controls

The Internal audit presented the report and explained that the audit had looked at proposals to manage out-of-hours cover, but the main bulk of the audit looked at patching and vulnerability, MFA, staff training and awareness and the mock "phising" exercise. A green level of assurance was concluded noting that all controls had been put in place. Despite this level of assurance, it was pragmatic to always assume that a cyber-attack could happen. Three recommendations were made and are detailed in the report.

6.3 Payroll Arrangements

The Internal audit presented the report and confirmed a positive outcome with a green level of assurance for this cyclical audit which is a significant one covering the largest area of revenue expenditure. Two low-priority and one medium-priority actions were flagged.

6.4 Progress Report

The Internal audit presented the report the progress report and explained that it provided an update on the delivery of the current year's Internal Audit Plan. She explained that report included briefings, including "Be Scam Savvy", and a "HE Briefing", which was timely as this flags changes to HE funding and assessment, suggesting that some modelling could be helpful to manage these significant changes and where OfS [Office for Students] has conducted a consultation process. It was suggested that a meeting with RSM be set up to share information on this important area and the impact of the changes. **Action**

Q. Would it be helpful to share the OfS Consultation Documents reference?

A. Yes – RSM will share some summary presentation slides on this with the Director of Risk, Control & Compliance, which have an audit-perspective. **Action**. It was noted that the full consultation documents were also available.

6.5 Benchmarking Information 2020-2021

The Internal audit presented the report presented the 2020/21 benchmarking report.

6.6 Internal Audit Plan 2022-2023 – initial discussion

Discussion took place regarding planning for the internal audit work for 2022/23, so that the Plan could be drafted in liaison with EMT and presented to the June Audit Committee meeting.

The Internal Auditor showed the six-year audit plan for the college, from 2018-2019. It highlighted suggested areas that were due for audit. The following areas were also discussed for inclusion:

- Equality, Diversity and Inclusion
- AoC Code of Governance (could be linked to EDI above)
- Careers and Employability.

The Chair requested that the Committee be invited to input to the draft report, once produced following the meeting between the Auditor and EMT. **Action**.

7. Health and Safety Termly Update

The Vice Principal presented the report and she noted that the number of accidents had risen, due to all students and staff now being back in college. There were no particular areas of concern to highlight.

8. Additional Audit Work

This item was deemed confidential.

9. Performance of External Auditors

This item was deemed confidential.

10. Management Report on Implementation of Recommendations

The Management Report on Implementation of Recommendations was received for information.

11. Date of the next meeting

The next meeting was scheduled for Tuesday 14th June 2022 at 6pm.

The Chair thanked Members and Staff for their attendance and contributions to the meeting.

The meeting ended at 7pm

Signed   Date **14 June 2022**

Signed by Amirun Nehar, acting Chair for this meeting

Confidential Minutes of the Audit Committee meeting held on 14 March 2022, online by Teams
starting at 6.00 pm

Present	Lucy Lee (Chair)
	Lindsey Stewart (Acting Principal)
	Geraldine Swanton
	Sarah Horton-Walsh
	Amirun Nehar (External Member)
In Attendance	Heather Evans (Vice Principal Finance)
	Pete Haynes (Vice Principal HR and Student Services)
	Sam Bromwich (Director Control & Compliance)
	Theresa Lynch (Clerk)

8. Additional Audit Work

9. Performance of External Auditors