

**Minutes of the Audit Committee held on Friday 29 November 2019 at 08.00 am in
Room 814 on the 8th floor of the Matthew Boulton Campus**

MINUTES

Present:	Apologies:
Simon Thompson (Chair) (ST)	
Michele Larmour (ML)	
Helen Miles (HM)	
In attendance:	
Cliff Hall	
Sir Dexter Hutt	
Louise Jones (LJ)	
Martin Penny (MP)	
Fiona Yardley (FY)	
Hilary Barber (HB)	
Tony Felthouse (TF) KPMG	
Alison Rowe (AR) BDO	
Rachel Jones (RJ) Item 2 only	
Alison Jones (AJo) Item 10 only	
<p>Apologies for absence No apologies for absence were received.</p> <p>ST welcomed HM to the meeting and introductions were made.</p>	
<p>Declarations of Interest There were no declarations of interest reported in addition to those recorded on the register of interests.</p>	
Item 1	<p>Minutes of the meeting held on 28 June 2019 The minutes of the last meeting were accepted as a true and accurate report subject to the addition of ML to the list of attendees.</p> <p>Resolved: That the minutes should be accepted subject to the amendment noted above.</p> <p>Matters arising and Action Log It was noted that all actions were completed with the exception of the Remuneration committee meeting. This will be scheduled for early 2020.</p>
Item 2	<p>JISC Cyber Security Penetration Report RJ presented the report circulated with the agenda highlighting the following:</p> <ul style="list-style-type: none"> ▪ External penetration and phishing testing is being undertaken annually by JISC. ▪ A significant risk comes from inappropriate actions by staff opening or responding to phishing emails. ▪ The report contains an outline of issues that have occurred during the year and actions taken to mitigate the risk. ▪ The report details a new Sharepoint site which, once implemented next summer, will increase the ability to mitigate risk. ▪ All critical, high and medium issues identified in the testing have been addressed.

	<ul style="list-style-type: none"> ▪ Self-assessment checks are run internally. ▪ The next level of testing will include college security processes, e.g. how easy it would be to access the building – and potentially systems – without the relevant ID. <p>ST invited questions.</p> <ul style="list-style-type: none"> ▪ ML noted the challenge of legacy systems which provide limited opportunity to mitigate risk. ▪ ST asked if the cyber threat is targeted or non-targeted. RJ responded that it is targeted and that issues have arisen when students have wanted to take the internet down. In one situation this action became the subject of a criminal prosecution with a student formally cautioned (although it was acknowledged that the student identified was probably not the main instigator). Other attempts have been made to access the HR and finance systems to change bank details. As a result a more secure system requiring one to one conversations for changes of this sort has been adopted. <p>RJ noted that it was clear at a recent Cyber Conference hosted by the college that BMet had been subject to less attacks than other local colleges and these had been quickly resolved with minimal impact on users.</p> <ul style="list-style-type: none"> ▪ ST asked if any link between the Prevent strategy and the outcomes of the Penetration testing had been identified. RJ responded no link had been noted and the college used Vsigo software to identify attempts to access inappropriate websites or searches. ▪ ST asked if there was any indication that attacks on the college were being used as a route to other governmental organisations and RJ confirmed this was not the case. ▪ ST asked about the timing of attacks and RJ replied that they were all within office hours, it being assumed that attackers were looking for maximum impact. However, RJ reassured governors that the IT department receive alerts in the event of an issue being raised and are able to respond on a 24/7 basis. ▪ DH asked who has access to system passwords. RJ confirmed that it was individuals only with some limited administrative access by the IT team. Passwords have to be changed regularly and later this year when the switch to Windows 10 takes place a further level of security will be implemented. RJ noted that any member of staff giving a password to students would be the subject of a disciplinary process. <p>RJ was thanked for her report.</p> <p>RESOLVED: That the Cyber Security Report should be noted.</p>
<p>Item 3</p>	<p>Internal Audit Annual Report 2018/19 AR presented her report which detailed the eleven areas reviewed as part of the 2018/19 internal audit programme.</p> <p>It was noted that these areas and the outcomes were discussed at the meeting held of the Audit committee on 28 June 2019.</p> <p>RESOLVED: That the Internal Audit Annual Report 2018/19 be noted.</p>
<p>Item 4</p>	<p>Subcontractor Audit Report AR reported that this audit had been carried out during June/July to meet new ESFA regulations associated with Sub Contractor provision. AR noted that the audit took place following a restructure of the Partnership team and the seven key findings of the audit were related in the main to this transition period. Management responses have been received by BDO to all issues identified and a certificate has been signed and issued in relation to the audit work.</p> <p>HM asked if the audit findings represented a legacy issue or are current practices not fully compliant. MP explained that they were a mixture of both. However, controls have changed significantly in line with ESFA regulations around Subcontractors and consequently a report will be presented to the Finance Committee at their meeting next week. MP noted it is now a strict requirement that the College website contains clear information about Subcontracting, eg the costs, how the costs are calculated, why subcontractors are being employed with supporting evidence being available. Subcontracting is now included in the Audit Action Log and the review has led to some refining of processes.</p>

	<p>Details of further discussion are included in the confidential minutes.</p> <p>RESOLVED: That the Subcontractor Audit Report be noted.</p>
Item 5	<p>Audit Committee Annual Report 2018/19</p> <p>MP presented the report explaining that its purpose is to ensure that the Audit committee works effectively, meets its Terms of Reference and fulfils statutory requirements. He emphasised that the report is owned by the committee and must comply with the Code of Good Governance.</p> <p>HB pointed out that the majority of actions noted as “Partially” completed are those relating to strategic planning. It was noted that the governors’ planning day took place on 07 November 2019 and LJ is leading the planning resulting from discussions held, with a view to a plan being brought to governors at the first Corporation meeting in the new year and implemented in the spring.</p> <p>ML commented on the assurance that the committee could now have (see point 15.6 of the report) that previous issues around budget setting and budgetary control have now been addressed. DH agreed that the report evidenced a “sea change” from the previous report.</p> <p>RESOLVED: That the Audit Committee Annual Report 2018/19 be recommended to the Corporation for approval.</p>
Item 6	<p>Regularity Audit Questionnaire</p> <p>MP presented the report which is part of the annual audit cycle and submitted to the external Auditors to support their overall assurance framework. Once reviewed by the Audit committee and approved by the Corporation it will be signed off by the Accounting Officer and the Chair of the Corporation.</p> <p>Details of further discussions are included in the confidential minutes.</p> <p>RESOLVED: That the Regularity Audit Questionnaire is approved.</p>
Item 7	<p>Draft Management Letter and Letter of Representation and Statement of Governance (Financial statement appended)</p> <p>This item is recorded in the confidential minutes.</p>
Item 8	<p>Annual Internal Audit Plan – 2019/20</p> <p>MP noted that agreement of the plan was obtained by email between meetings. The audit will begin on Monday 09 December.</p> <p>RESOLVED: That the plan should be recommended to the Corporation for approval.</p>
Item 9	<p>Risk Register update</p> <p>MP introduced the Risk Register pointing out that its purpose was to identify both ongoing risks that needed mitigation and also “live” risks which may be short or longer term. The register is compiled in conjunction with LJ and checked against action/recovery plans to ensure all issues are covered in the register. Active risks include succession planning for SLT and for governors.</p> <p>MP noted that the risk register is a “live” document and reviewed on a monthly basis by SLT to ensure risks are included as necessary and that items can be removed.</p> <p>The RAG rating is self-assessed; however although staff who own the risk can add the actions they have taken, the RAG colour can only be changed by a member of executive staff once they have scrutinised the actions taken.</p>

	<p>It was agreed that MP/LJ would add a colour key to the document.</p> <p>HM commented that it was positive that it was possible to remove some issues from the register but acknowledged that some items, eg funding would remain a high risk as the college cannot control this.</p> <p>ML asked who has ownership of the register. MP confirmed that he had this responsibility on behalf of the Principal. It is quality assured by SLT and CH. Risks are owned by members of SLT.</p> <p>RESOLVED: That the committee note the Risk Register.</p>
<p>Item 10</p>	<p>Internal Audit Reports</p> <p>(i) Progress Report to include update from HR Director</p> <p>MP presented the Audit Tracker showing the current list of actions required, some of which are complete and others due for completion by the end of November. Individuals can update the last two columns but only the executive team can amend the RAG rating once evidence of action taken is on file. DH suggested that the inclusion of a note to this effect would be helpful for governors. It was noted that auditors will have access to the evidence file as part of their testing.</p> <p>ST asked what would constitute a red rating and MP explained this would be where no action or update had been noted and the deadline missed. Such items will be referred to SLT.</p> <p>AJo joined the meeting and reported to the committee on the 4 HR aspects of the tracker which were completed earlier in the year as part of the HR audit, ie numbers 15,16,19,20.</p> <p><i>Item 15 – Vetting Checks Policy</i> The policy has been refreshed and reviewed and approved by SLT. It has been shared with staff.</p> <p><i>Item 16 - Staff Recruitment</i> The recommendation was to ensure documentation was incorporated into the policy. This has been actioned and additionally new processes are in place that require all completed recruitment information and paperwork to be returned to HR for confidential record keeping. All processes have been approved by SLT.</p> <p><i>Item 19 – Vacancy Request Form</i> The process has been refreshed and the future aspiration is for the IT team to implement an online process. In the meantime staff are operating in accordance with a paper based process.</p> <p><i>Item 20 – Induction Policy</i> The induction checklist has been aligned to the policy and once completed supporting documents are returned to HR.</p> <p>Ongoing actions:</p> <ul style="list-style-type: none"> • Draft formal Performance Development and Reward policies are with MP and LJ for review prior to being submitted to SLT in December • Probation process: To meet the recommendation that probation monitoring dates need to be clearer, the college will revert to a paper system from the start of the new year to log these until an online system can be identified • The recommendation from previous audits (Item 2) to enter into a Framework Agreement has now been completed. The contract is with Morgan Hunt and offers reduced rates for both agency staff and permanent recruitment. • Payroll and expenses audit: this related to how additional hours worked are recognised. There are two schemes in operation, hourly paid staff can work additional hours subject to approval of timesheets and a TOIL Policy is in place which covers how other staff can reclaim additional hours worked <p>AJo invited questions.</p> <p>Further discussion is included in the confidential minutes.</p> <p>AJo was thanked for her update and left the meeting.</p>

	<p>RESOLVED: That the Internal Audit Report be noted.</p>
Item 11	<p>Insurance Annual Report Questions were invited from governors. FY confirmed that the insurance valuation had been updated and checked against current cover.</p> <p>RESOLVED: That the Insurance Annual Report be noted.</p>
Item 12	<p>Health and Safety Report ST noted a slight increase in RIDDOR incidents but none that raised any major concerns.</p> <p>ST congratulated all staff involved in maintaining Health and Safety standards for the low occurrence of issues.</p> <p>RESOLVED: That the Health and Safety Report be noted.</p>
<p>ST thanked all present for attending the meeting and their contributions. The meeting concluded at 10.00 am.</p>	
<p>Date of next meeting: Friday 06 March 2020</p>	

Simon Thompson

Signed: [Simon Thompson \(Jul 28, 2020 16:32 GMT+1\)](#)

Chair: Simon Thompson

BMet Audit Minutes - 29 November 2019 - TO BE SIGNED

Final Audit Report

2020-07-28

Created: 2020-07-24
By: leona.fisher@bmet.ac.uk
Status: Signed
Transaction ID: CBJCHBCAABAangaMmfYEnW-WbnGkckKf76vJIIAYrqna



"BMet Audit Minutes - 29 November 2019 - TO BE SIGNED" History



Document created by leona.fisher@bmet.ac.uk

2020-07-24 - 15:43:35 GMT- IP address: 212.219.40.2



Document emailed to Simon Thompson (simothompson@deloitte.co.uk) for signature

2020-07-24 - 15:44:18 GMT



Email viewed by Simon Thompson (simothompson@deloitte.co.uk)

2020-07-28 - 11:13:10 GMT- IP address: 148.252.133.191

Document e-signed by Simon Thompson (simothompson@deloitte.co.uk)

Signature Date: 2020-07-28 - 15:32:11 GMT - Time Source: server- IP address: 86.22.23.156

Signed document emailed to leona.fisher@bmet.ac.uk and Simon Thompson (simothompson@deloitte.co.uk)

2020-07-28 - 15:32:11 GMT