G

AUDIT COMMITTEE REPORT

Subject: Internal Audit Assignment – Follow-Up Review	**Purpose:** **For Approval** ☒ **For Discussion** ☐ **For Information** ☐
Prepared by: Peter D Smith, Vice Principal – Finance and Resources	**Date:** 04 May 2017

Purpose: To consider the findings of the internal audit Follow-Up Review and approve the management responses and any further actions.

Linked to Strategic Goal 3: Provide a high quality College experience.

Executive Summary:

Attached is the Internal Auditor's report on the Follow-Up Review of previous assignments. The report concludes that: -

"*the College has endeavoured to implement recommendations as far as possible. In areas where recommendations have not been fully implemented, the College are still considering these in line with ongoing business and development.*"

Recommendation: Committee are invited to consider and approve the report and management response, with further actions as necessary.

Previous Committee Approvals: n/a

For publication ☒	**For publication with redactions** ☐	**Not for publication** ☐

Signed:

Vice Principal – Finance and Resources

Wylie+Bisset
Chartered Accountants, Business & Tax Advisers

Borders College

Internal Audit 2016/17

Follow Up Review

February 2017

Overall Conclusion
Substantial

TABLE OF CONTENTS

Section		Page
1.	Executive Summary	3
2.	Audit Arrangements	6
Appendices		
A.	Not Implemented Recommendations	8
B.	Partially Implemented Recommendations	14
C.	Fully Implemented Recommendations	25
D.	Grading Structure	32
E	Assignment Plan	34

The matters raised in this report came to our attention during the course of our audit and are not necessarily a comprehensive statement of all weaknesses that exist or all improvements that might be made.

This report has been prepared solely for Borders College's individual use and should not be quoted in whole or in part without prior written consent. No responsibility to any third party is accepted as the report has not been prepared, and is not intended, for any third party.

We emphasise that the responsibility for a sound system of internal control rests with management and work performed by internal audit should not be relied upon to identify all system weaknesses that may exist. Neither should internal audit be relied upon to identify all circumstances of fraud or irregularity should there be any although our audit procedures are designed so that any material irregularity has a reasonable probability of discovery. Even sound systems of control may not be proof against collusive fraud. Internal audit procedures are designed to focus on areas that are considered to be of greatest risk and significance.

1 EXECUTIVE SUMMARY

Purpose of Review

The purpose of the review was to assess whether the College has appropriately implemented the internal audit recommendations made in 2015/16 and earlier years. Our review considered whether any issues are outstanding beyond the agreed implementation deadline.

Our review considered all outstanding recommendations to provide the Board, via the Audit Committee, with independent assurance that we are satisfied that these recommendations have been fully implemented by the College and can therefore be removed from the audit action plan.

This assignment is part of the agreed 2016/17 Annual Internal Audit Plan for the College.

Scope of Review

Our objectives for this review were to ensure:

- The College has appropriately implemented any outstanding internal audit recommendations made in prior years.

Our approach to this assignment took the form of discussion with relevant staff, review of documentation and where appropriate sample testing.

1 EXECUTIVE SUMMARY

Conclusion

Overall Conclusion: Substantial

We can conclude that the College has endeavoured to implement recommendations as far as possible. In areas where recommendations have not been fully implemented, the College are still considering these in line with ongoing business and development.

Summary of Recommendations

Grading of Recommendations	High	Medium	Low	Total
Appendix A – Not Implemented Recommendations	-	2	4	6
Appendix B –Partially Implemented Recommendations	-	3	6	9
Appendix – Fully Implemented Recommendations	2	2	2	6

Implementation of Recommendations

Summary of Implementation					
Audit Area	**Total**	**Not Implemented**	**Partially Implemented**	**Superseded**	**Fully Implemented**
Follow up review (January 2016)	12	2	5	-	5
Corporate Governance (January 2016)	2	1	1	-	-
Performance Management & Review (January 2016)	1	-	-	-	1
MIS Department (March 2016)	3	2	1	-	-
Student Funding Application System (June 2016)	3	1	2	-	-
Total	**21**	**6**	**9**	**-**	**6**
Percentage of Total	**100%**	**29%**	**43%**	**-**	**28%**

2 AUDIT ARRANGEMENTS

The table below details the dates of our fieldwork and the reporting of the audit area under review.

Audit Stage	Date
Fieldwork start	13 February 2017
Closing meeting	17 February 2017
Draft report issued	3 March 2017
Receipt of management responses	27 April 2017
Final report issued	28 April 2017
Audit Committee	18 May 2017
No of audit days	2

2 AUDIT ARRANGEMENTS

We detail below our staff who undertook the review together with the College staff we spoke to during our review.

Wylie & Bisset LLP			
Partner	Ross McLauchlan	Partner	ross.mclauchlan@wyliebisset.com
Director	Graham Gillespie	Director of Internal Audit	graham.gillespie@wyliebisset.com
Manager	Stephen Pringle	Senior Internal Audit Manager	stephen.pringle@wyliebisset.com
Lead Auditor	Ricky Meechan	Internal Audit Senior	ricky.meechan@wyliebisset.com
Auditor	Scott McCready	Internal Audit Assistant	scott.mccready@wyliebisset.com

Borders College			
Key Contact	Pete Smith	Vice Principal - Finance & Resources	psmit@borderscollege.ac.uk

Wylie & Bisset appreciates the time provided by all the individuals involved in this review and would like to thank them for their assistance and co-operation.

Appendix A

Not Implemented Recommendations

Not Implemented Recommendations

(Business Impact Analysis, Student Funding Application System, June 2016)

Original Finding
Through discussion with the Student Funding Manager, we identified that there has been no business impact analysis carried out with regard to the Student Funding Online Application System (CAMS). This would determine the consequence of data loss or the system being unavailable for a period of time which would lead to an agreed acceptable downtime and an agreement on how often data should be backed up. During our review the Student Funding Manager queried with the IT department how often the CAMS data is backed up and was informed that this was 1 incremental backup a day. On reflection of this information it was felt that the backup windows should be increased as 1 day was considered unacceptable data loss if there was a need to restore.

Original Recommendation
We recommend that the College carry out a business impact analysis for the CAMS system to ensure there is an agreed backup window and acceptable downtime for the system. We would encourage this analysis to be carried out for all College systems to ensure there is a formal agreement for the prioritisation and backup of services, which would change, depending on the time of the year.

Original Management Response
I agree that a daily backup is not sufficient when this is a live system used by customers out with the establishment. As part of a disaster recovery plan we will carry out a business impact analysis and review the frequency of backups.

Ref	Finding from our 2016/17 Follow Up	Grade	Recommendation
1	No work has been carried out since our last review regarding how often the College's key systems should be backed up. The backup window for the CAMS application system is still 1 day which was deemed unacceptable by the Student Funding Manager.	**Medium**	We repeat our original recommendation.

Management Response	Responsibility and Implementation Date
Agreed. Head of ISLT has been liaising with Lead Auditor to agree format of analysis report	*Responsible Officer: Head of ISLT* *Implementation Date: 30 June 2017*

Not Implemented Recommendations

PIN Codes Smart Devices (IT Systems – May 2014)

Original Finding
The College do not force the use of PIN codes on smart devices such as smart phones or tablets that connect to the College network.
Original Recommendation
We recommend the College ensure smart devices are connected with security PIN codes. There are a number of ways to do this, most commonly this is enforced through smart devices connecting to the Exchange server which can be configured to require a PIN code before connections are allowed.
Finding from our Follow Up 2014/15
With the development of the 'Bring Your Own Device' scheme, the College are still in the process of considering how this recommendation would be implemented in practice.
Recommendation from our Follow Up 2014/15
We repeat our original recommendation.
Finding from our 2015/16 Follow Up
The Head of ISLT advised that the College are not planning on implementing PIN codes as part of security. This recommendation was treated as Superseded in our last review however, the Audit Committee instructed that the recommendation should be implemented.

Ref	Finding from our 2016/17 Follow Up	Grade	Recommendation
2	The Head of ISLT advised that they were in the process of phoning all staff with a College mobile phone to instruct them to enforce a PIN code. We advised the Head of ISLT that PIN codes can be forced on mobile devices via the College's email server. We were informed that the College will now look to do this as soon as possible.	**Medium**	We repeat our original recommendation.

Management Response	Responsibility and Implementation Date
Agreed. Audit of current devices carried out and staff advised of requirement to have PIN codes.	*Responsible Officer: Head of ISLT* *Implementation Date: 30 June 2017*

Not Implemented Recommendations

(Online Applications, MIS Department, March 2016)

Original Finding
Online applications are only available for full time and some part time courses. BDU, certain part time, school and evening courses cannot be applied for online. For courses with no online application, students go straight to enrolment. Enrolment without pre-application may lead to inefficiency as staff do not have pre-entered information available from the application and must then enter this manually.

Original Recommendation
We recommend that the College consider introducing an online application process for all courses on offer.

Original Management Response
Agreed. This has been raised at ISLT Strategy Committee and will be taken forward by the Web Technologies Group. Head of ISLT and Head of MIS will come back with recommendations once this has been looked at further.

Ref	Finding from our 2016/17 Follow Up	Grade	Recommendation
3	This recommendation has not been implemented as yet. The College has stated that they are awaiting the announcement of the Scottish Funding Council's funding allocations which is due to be announced in Spring 2017.	Low	We repeat our original recommendation.

Management Response	Responsibility and Implementation Date
Agreed. The College agrees this is important; however, other systems developments have been agreed as taking precedence.	*Responsible Officer: Head of MIS / Head of ISLT* *Implementation Date: 30 June 2018*

Not Implemented Recommendations

(Conflicts of Interest, Corporate Governance, January 2016)

Original Finding
Through our review we found that there are two student members of the Board of Management for whom a registers of interest form is not held.
Original Recommendation
We recommend that register of interest forms are completed on an annual basis by all board members, including staff and student members.
Original Management Response
Agreed. Due to the timing of appointments, an annual update does not always cover staff and student members. Procedures will be amended to ensure all members' interests are updated.

Ref	Finding from our 2016/17 Follow Up	Grade	Recommendation
4	The Register of Interests document which is published on the College website, does not contain the interests of the 2 student members of the Board of Management and the interest of the new Principal.	Low	We recommend that the College ensure that registers of interests are obtained for all Board of Management members. We also recommend that the document is updated on the website.

Management Response	Responsibility and Implementation Date
Agreed. This will be implemented.	*Responsible Officer: Clerk to the Board* *Implementation Date: 30 April 2017*

Not Implemented Recommendations

IT Security Policy (IT Systems – May 2014)

Original Finding
The IT security policy is due to be updated, this should also include sections on third party access and access control and explain in more detail the physical and network security in place to protect the College systems.

Original Recommendation
We recommended the policy is updated to cover the following areas or explain them in more detail; third party access, remote access, access control physical and network security. Alternatively there could be separate policies for each area.

Finding from our 2014/15 Follow Up
The IT Security Policy remains a work in progress. The College has been working on the content of the policies however has still to decide on a suitable structure for the new policy/policies.

Finding from our 2015/16 Follow Up
This policy has not yet been finalised and approved by the Board.

Ref	Finding from our 2016/17 Follow Up	Grade	Recommendation
5	Through discussions with the Head of ISLT we were informed that the creation and updating of the current IT Security Policy has been put on hold due to the implementation of a new IT infrastructure being recently approved. The policy will be updated once this implementation is complete.	Low	We repeat the original recommendation.

Management Response	Responsibility and Implementation Date
Agreed. This will be completed as part of infrastructure improvements.	*Responsible Officer: Head of ISLT* *Implementation Date: 31 July 2017*

Not Implemented Recommendations

(Student Certification, MIS Department, March 2016)

Original Finding
The Unit E system used by MIS is not set up to link automatically with the systems used by all awarding bodies to allow entries and results to be processed electronically. There is duplication of work involved in the certification of non-SQA students as these need to be manually re-keyed into the system of the other awarding bodies. SQA results are currently automatically updated from the Unit-e system.
Original Recommendation
We recommend that the College explore the possibility of setting up the Unit-e system to allow electronic transfer of files with all awarding bodies.
Original Management Response
Agreed. There is some exploratory work underway and Head of ISLT and Head of MIS will come back with recommendation once this work has progressed further.

Ref	Finding from our 2016/17 Follow Up	Grade	Recommendation
6	This has been discussed but no work has yet been started on this as Capita (Unit-e software vendor) are re-writing a part of the UNIT-e system which may address this. A new revised date has been set by the College, following feedback from SQA on their system timescales.	Low	We repeat our original recommendation.

Management Response	Responsibility and Implementation Date
Agreed. This will be progressed as part of the national Awarding Body to Centre Project.	*Responsible Officer: Head of MIS* *Implementation Date: 31 December 2018*

Appendix B

Partially Implemented Recommendations

Partially Implemented Recommendations

Estates Strategy (Estates Management, January 2015)

Original Finding
Through our review we identified that the College does not have a formally documented Estates Strategy. From our discussions with the Director of Finance & Estates we understand that the College are in the process of finalising the direction in which they intend to follow prior to finalising an Estates Strategy.
Original Recommendation
We recommend that the College finalise the direction in which they intend to move and formally document their Estates Strategy.
Finding from our 2015/16 Follow Up
The preparation of the Estates Strategy has been put on hold in order for it to be produced in conjunction with the College's new Corporate Plan.
Recommendation from our 2015/16 Follow Up
We repeat the original recommendation.

Ref	Finding from our 2016/17 Follow Up	Grade	Recommendation
1	The Estates Strategy is now in early draft stage. The College has set a new revised date of June 2017.	Medium	We recommend the College review and issue the draft Estates Strategy.

Management Response	Responsibility and Implementation Date
Agreed. Estates Strategy scheduled for consideration by Board in June 2017	*Responsible Officer: Vice Principal - Finance and Resources* *Implementation Date: 30 June 2017*

Partially Implemented Recommendations

Web-filtering Protection (IT Systems, May 2014)

Original Finding
The College currently are not filtering internet traffic on the College guest wireless network. This should filter the likes of pornography and offensive websites if being made available by the College, to protect the College's reputation. Also the College do not fully utilise the Barracuda web filtering solution to block the downloading of dangerous file types on the main production network, this would provide better security to eliminate rogue and infected files from being downloaded and run on the College systems.

Original Recommendation
We recommend the College introduce web filtering on any wireless networks being made available. We also recommend the College utilise the blocking of dangerous file types via the Barracuda web filtering solution.

Finding from our 2014/15 Follow up
Our retesting of the guest wireless network found that offensive images could still be accessed. From discussions with the Head of ISLT, we understand that the College are currently utilising the maximum security available on the product used on the guest network. The College has considered the blocking of specific file types however consider that in doing so would impede the teaching of computing courses. The College are satisfied that their web-filtering and anti-malware products would block any infected/dangerous files from being downloaded and run on the College systems.

Finding from our 2015/16 Follow Up
This point is to be investigated further in order to facilitate appropriate filtering for the online services provided to Heriot Watt University who give full academic freedom to their students.

Ref	Finding from our 2016/17 Follow Up	Grade	Recommendation
2	The College's Finance and General Purposes Committee has now approved the award of a new ISLT infrastructure to be implemented. A new web-filtering system will be implemented as part of this infrastructure and will applied to all wireless networks.	**Medium**	We recommend that the web-filtering system is applied to all wireless networks once the new ISLT infrastructure is implemented.

Management Response	Responsibility and Implementation Date
Agreed. To be implemented as part of infrastructure renewal.	*Responsible Officer: Head of ISLT* *Implementation Date: 31 July 2017*

Partially Implemented Recommendations

(Course Information, MIS Department, March 2016)

Original Finding
Information on curriculum content received by the MIS team from each faculty often varies in format and is at times delayed or slow. The mix of information received makes it very difficult for the MIS department to build the information on the system quickly and the delays in receiving the information required slows the process down. As a result, at times the curriculum may not be built in time for enrolment. Rushing of the process also increases the likelihood of human error.
Original Recommendation
We recommend that the College develops a standard information entry tool to be used by all faculties.
Original Management Response
Agreed. Head of MIS and Systems Developer are currently working on a tool to do this which will be shared with other relevant staff when it is at an appropriate stage to do this.

Ref	Finding from our 2016/17 Follow Up	Grade	Recommendation
3	This tool is in the early stages of testing and still to be shared with Faculty Heads. Therefore, we have treated this recommendation as being partially implemented.	**Medium**	We recommend that the College implement the entry tool once testing is completed and satisfactory.

Management Response	Responsibility and Implementation Date
Agreed. An interim solution is in place and further work will be carried out as resources are identified, with the intention to fully implement for Academic Year 2018-19.	*Responsible Officer: Head of MIS / Head of ISLT* *Implementation Date: 31 July 2018*

Partially Implemented Recommendations

Raising Purchase Orders (Financial Controls - April 2013)

Original Finding
Our review found that the lecturers of the College do not all have access to the PECOS system. Instead the raising of orders is processed by a designated requisitioner for each department. We found that there was no consistent method for lecturers to request purchase orders are raised in PECOS which could lead to lecturers spending time looking up items on suppliers websites/catalogues and either emailing or verbally discussing the order with the designated requisitioner. This process is not really providing the College with the time savings it had hoped to achieve.
Original Recommendation
We recommend that all lecturers are provided with access to the PECOS system. This will allow the lecturer to select the item they wish from the PECOS catalogue and raise the order immediately thus reducing time spent reviewing and discussing orders with requisitioners.
Finding from our Follow Up 2013/14
The College have recently undertaken a trial where access to the PECOS system was provided to lecturers in one of the College's faculties. The results of the trial are currently being assessed. The College will then make a decision on whether access should be rolled out to all lecturers.
Recommendation from our Follow Up 2013/14
We recommend that the College complete their assessment of the trial and make a decision on which members of staff should be provided with access to the PECOS system.
Finding from Follow Up 2014/15
The assessment of the trial was completed and a decision was made that PECOS should be rolled out college wide. Roll out however has been delayed due to the departure of the College's Procurement Officer in January 2015.
Recommendation from Follow Up 2014/15
We recommend that once a new Procurement Officer has been appointed, the College roll out PECOS college wide.
Finding from our 2015/16 Follow Up
The rollout of access to the PECOS system is an on-going process. There has been an increase in the lecturers access but this has not as yet been rolled out college wide.

Ref	Finding from our 2016/17 Follow Up	Grade	Recommendation
4	The phased implementation of the PECOS system throughout the College continues.	Low	We recommend that the College continue with the phased implementation to ensure this is implemented College wide.

Management Response	Responsibility and Implementation Date
Agreed. PECOS implementation will continue to be extended.	*Responsible Officer: Head of Finance and Procurement* *Implementation Date: 30 July 2017*

Partially Implemented Recommendations

Endpoint Control Solution (IT Systems - May 2014)

Original Finding
The current situation in the College is that any user can copy data to removable media such as a USB drive and take this off site.
Original Recommendation
We recommend the College investigate the use of an Endpoint control solution to provide control over data leaving the College network via removable media.
Finding from our Follow Up 2014/15
The College is still investigating whether an Endpoint control solution is a suitable solution.
Recommendation from our Follow Up 2014/15
We repeat our original recommendation.
Finding from our 2015/16 Follow Up
The Head of ISLT has advised that a decision has been made by the College that an endpoint control solution will not be purchased.
This recommendation was treated as Superseded in our last review however, the Audit Committee instructed that the recommendation should be implemented.

Ref	Finding from our 2016/17 Follow Up	Grade	Recommendation
5	The Head of ISLT has advised that the College are investigating possible solutions to provide more control over sensitive data being leaked from the network.	Low	We recommend the College continue to investigate possible solutions and following this implement this to ensure controls are in place.

Management Response	Responsibility and Implementation Date
Agreed. A recommendation will be made to management following completion of infrastructure project.	*Responsible Officer: Head of ISLT* *Implementation Date: 31 July 2017*

Partially Implemented Recommendations

Manual Systems (Staff Utilisation, March 2015)

Original Finding
Through our review we found that the current processes in place for the creation of the College's timetables are somewhat manual and time consuming. The Heads of Faculty currently prepare the timetables for their own faculty and we found that the approaches taken in building the timetables are not consistent across the College. We consider that the current processes employed in creating the timetables involves a considerable amount of duplication of effort in order to provide the various support departments with the information they require.
We do note that the College are currently in the process of evaluating its timetabling processes and have set up two consultation groups - one to look at the timetabling process to see where improvements can be made and one to consider the requirements for an automated timetabling system.
Original Recommendation
We recommend that the College seek to streamline the timetabling processes and roll out a less onerous and consistent approach across the College.
Finding from our 2015/16 Follow Up
The process for preparing timetables has been altered in that the faculty heads now begin with the same template, however after discussion with Vice Principal Curriculum it seems that any amendments to timetables are still extremely time consuming, therefore more work must be done in order to streamline this process.

Ref	Finding from our 2016/17 Follow Up	Grade	Recommendation
6	We were informed by the College that systems have been explored and are currently testing a system from Celcat but are awaiting the Scottish Funding Council allocation which is due in Spring 2017.	Low	We repeat the original recommendation.

Management Response	Responsibility and Implementation Date
Agreed. CELCAT has been purchased and will be implemented for 2017-18.	*Responsible Officer: Head of ISLT* *Implementation Date: 31 July 2017*

Partially Implemented Recommendations

(Self-Evaluation, Corporate Governance, January 2016)

Original Finding
We note that there is currently no annual self-evaluation carried out by the Chair of the Board or Chairs of the individual sub-committees. This means that the performance of the Board and Committee chairs' is not assessed and as such it is difficult to assess whether the Chairs are effective in their roles.

Original Recommendation
We recommend that the Chair of the Board and Chairs of each sub-committee complete a self-evaluation on an annual basis. The evaluation should normally be led by the Vice Chair of the Board/Committee.

Original Management Response
Agreed. Self-evaluation of the Chairs of Board and Committee will be added to the annual self-evaluation schedule.

Ref	Finding from our 2016/17 Follow Up	Grade	Recommendation
7	This remains a work in progress. A questionnaire has been created by the College and is currently in draft form.	Low	We recommend that the College implement an annual self review of the Chairs of the Regional Board and Committees once the questionnaire has been approved.

Management Response	Responsibility and Implementation Date
Agreed. Process is currently under consideration by Chair and Clerk.	*Responsible Officer: Clerk to the Board* *Implementation Date: 31 July 2017*

Partially Implemented Recommendations

(Feedback Survey, Student Funding Application System, June 2016)

Original Finding
Through our review of the College's Learner Feedback Survey, we noted that the percentage of good feedback from students has dropped from 67% in 2014/15 to 44% in 2015/16, when answering the statement "It was easy to apply for a Bursary/EMA". However, it was noted that the majority of the comments left by students were not relevant to the online application system, for example there were complaints over there being too much information to provide, which is not a fault of the system. In discussion with the Student Funding Manager, it was explained that the department had also noted this and had stated that they were looking into the use of an online survey function, such as Survey Monkey, which would be specific to the online application system only. The departments thinking was to present this survey at the end of the application submission process.

Original Recommendation
We recommend that the College continue with plans to produce a survey that is specific to the online application system to get relevant feedback to make any necessary tweaks or improvements.

Original Management Response
We are currently considering the questions to be included in an online survey, a link to which will be included in the email issued on submission of an application. For the current academic year we will issue a separate email to students who have already submitted their application. This should ensure the responses are particular to the CAMS application system and not the policy surrounding processing of awards.

Ref	Finding from our 2016/17 Follow Up	Grade	Recommendation
8	The College are planning to encompass an automatic survey request following submission of the funding application. This is being developed and implemented for new applications for 2017 onwards. A new revised date of 31 May 2017 has been set by the College.	Low	We recommend that the College finalise the development and implementation of the feedback survey.

Management Response	Responsibility and Implementation Date
Agreed. Being developed and implemented for new applications for 2017 onwards. New revised date of 31 May has been set.	*Responsible Officer: Head of Student Services / Student Funding Manager* *Implementation Date: 31 May 2017*

Partially Implemented Recommendations

(Data Retention, Student Funding Application System, June 2016)

Original Finding
During our review we enquired whether the online application system was configured in line with data retention regulations and/or policies. We noted that there was no retention guidance in place for student applications.
Original Recommendation
We recommend that the College investigate what the retention requirements and regulations are for student funding applications and ensure that the application system is configured in line with these requirements.
Original Management Response
As discussed during our meetings, SFC recommends that a reasonable period to keep records on student support (Bursary, Childcare and Discretionary Fund) is one year after the student's period of support has ended. For EMA purposes, information (either electronic or paper) is to be retained for 6 years. However, documentation associated with ESF students is required to be retained until 2032.

We will write a policy which encompasses these rules and in what format the information should be retained. On expiry of the retention period, information will be destroyed.

Ref	Finding from our 2016/17 Follow Up	Grade	Recommendation
9	The College have drafted a policy and this is under review by the Senior Management Team.	Low	We recommend that the Policy is implemented and approved at the next Regional Board meeting.

Management Response	Responsibility and Implementation Date
Agreed. Meeting with SMT members and HoFs to review bursary/EMA policy with a view to incorporating all required info including retention of records.	*Responsible Officer: Head of Student Services / Student Funding Manager* *Implementation Date: 31 March 2017*

Appendix C

Fully Implemented Recommendations

Fully Implemented Recommendations

Self Assessment Questionnaire and Attestation of Compliance (PCI Compliance, March 2015)

Original Finding
We note that the College has not completed a Self Assessment Questionnaire (SAQ) or Attestation of Compliance (AOC) to confirm its compliance with PCI Data Security Standards. As a result, the service provider is currently charging the College a monthly fee of £9.99. More importantly however as the SAQ and AOC have not been completed, the College has therefore not confirmed its compliance with PCI DSS, and would be responsible for any losses incurred through fraud.
Original Recommendation
We recommend that the College completes the relevant Self Assessment Questionnaire and Attestation of Compliance as soon a possible.
Finding from our 2015/16 Follow Up
The Self Assessment Questionnaire has not yet been completed. Delays in the completion are due to a new head of ISLT being appointed who has been developing an understanding and knowledge of the College's system prior to completing the application.
Recommendation from our 2015/16 Follow Up
We repeat the original recommendation.

Ref	Finding from our 2016/17 Follow Up	Grade	Recommendation
1	The application has been submitted and a compliance certificate has been awarded.	High	No further action required.

Fully Implemented Recommendations

Sensitive Data Storage (PCI Compliance, March 2015)

Original Finding
Through our testing we found that there are primary account numbers (PANs) and sensitive card data being held by the College.
The merchant copy receipts printed from the College's card reader does not currently mask PANs. In line with PCI DSS, PAN numbers should be rendered unreadable with a maximum of the first 6 and last 4 digits displayed. We note that the College are currently masking PAN's unreadable using a tipex mouse; however on physical inspection of the receipts we found that the numbers could easily be reconstructed.
The College also use a 'Credit/Debit Card Payment Details Form' when the card machine does not work properly. These paper forms require the payee to fill out their card details including PAN and card verification code (CVC). We note through physical inspection of these, although PANs are being masked as above, the CVC is not being masked in any way. As the CVC is considered to be sensitive data, these should not be stored once the transaction has been completed. We do note that these forms are placed in the College safe as soon as the transaction has been completed.
The College also have a 'Community and Evening Class Application Form' which gives the option for the applicant to include their card details. Again this includes the PAN and CVC. We note that these are not being masked. These forms are stored in a locked cupboard within the Business Development Unit once the payment has been processed.
Original Recommendation
We recommend that the College ensure that where PANs are being held, the number is masked so that only a maximum of the first 6 and last 4 digits are readable. We would recommend that the College contact the card machine provider to request the settings on the card machine are changed so that the PANs included on the merchant copy receipts are masked. The College should ensure that where numbers are being masked manually, that the numbers are not able to be reconstructed.
We also recommend that the College reformats its 'Credit/Debit Card Payment Details Form' and 'Community & Evening Class Application Form' so that any sensitive information can be easily removed from the form and destroyed as soon as payments have been processed.
Finding from our 2015/16 Follow Up
The College has contacted the card machine provider to enquire whether it is possible to change the settings to mask the PANs, but were informed that it does not have this facility. In light of this, the College now use a thick black marker in order to render the PANs unreadable.
In terms of the 'Credit/Debit Card Payment Details Form' and the 'Community & Evening Class Application Form' there have been no changes to the format to allow PAN and CVC numbers to be easily removed and destroyed after the payments have been processed.

Ref	Finding from our 2016/17 Follow Up	Grade	Recommendation
2	The 'Credit/Debit Card Payment Details Form' and the 'Community & Evening Class Application Form' now have a tear off section which is destroyed as soon as payments are processed. Through sample testing we can confirm that all 5 slips tested had the appropriate section destroyed.	High	No further action required.

Fully Implemented Recommendations

Asset Management Training (Fixed Asset Management – May 2014)

Original Finding
We note that Faculty Heads are currently responsible for the management of any small items of equipment 'owned' by their faculty. During our review however we have been unable to obtain any inventory listings/records of the equipment held in any of the faculties.
Original Recommendation
We recommend that the College ensure that Faculty Heads, and those others responsible for the management of College assets/equipment are provided with training to ensure that they are fully aware of their responsibilities in relation to asset management.
Finding from Follow Up 2014/15
Faculty Heads have been reminded of their responsibilities and provided with a pro-forma asset register to record the equipment held in their faculty. Population of the asset registers is ongoing and it anticipated that this will be completed by the College year end.
Recommendation from Follow Up 2014/15
We recommend that the College ensure that the asset registers held by each faculty are complete by the due date.
Finding from our 2015/16 Follow Up
Fixed Asset Registers are available from all Heads of Faculty and have been prepared using a pro-forma register. This is only considered to be partially implemented as some of the registers are not yet fully complete.

Ref	Finding from our 2016/17 Follow Up	Grade	Recommendation
3	Through our review and discussion with the Head of Finance and Procurement we are able to confirm that all registers have now been completed.	Medium	No further action required.

Fully Implemented Recommendations

Removal of Leavers from IT systems (Human Resource Management, January 2015)

Original Finding
Through our sample testing of seven leavers in the year, we identified that the IT user accounts of two of these had not been disabled.
Original Recommendation
We recommend that the College ensure that IT user accounts are disabled for all leavers in a timely manner.
Finding from our 2015/16 Follow Up
From our further sample of 4 leavers we found that one user account had not been disabled.
Recommendation from our 2015/16 Follow Up
We repeat the original recommendation.

Ref	Finding from our 2016/17 Follow Up	Grade	Recommendation
4	Through our sample testing, we can confirm that all 5 leavers tested had their user accounts disabled. We can also confirm through our testing that the IT Department were notified before the staff member's employment had been terminated.	Medium	No further action required.

Fully Implemented Recommendations

Remote Access to Network Shares (IT Systems – May 2014)

Original Finding
The College allow users to connect to their files on the network via HTTPCommander. Initially this was so staff could access the home drive which would not contain sensitive data. Now staff are able to access and download College network shared drives which could contain sensitive data. The remote access is not over a secure connection and staff are able to download content onto unmanaged devices.
Original Recommendation
We recommend the College review and investigate the remote access solution and its capabilities and look to provide a more secure connection for staff to access College data. This would then be documented as part of the College's ICT security policy.
Finding from Follow Up 2014/15
We note that the HTTP Commander continues to be used to allow users to connect to their files on the network.
Finding from our 2015/16 Follow Up
The Head of ISLT, has agreed that this point should be carried forward to next year as he intends to investigate this area during 2016.

Ref	Finding from our 2016/17 Follow Up	Grade	Recommendation
5	We are able to confirm that the College's remote working solution is now running over HTTPS (HyperText Transfer Protocol over SSL (Secure Socket Layer)) which encrypts traffic to and from the machine connecting to the network remotely.	Low	No further action required.

Fully Implemented Recommendations

(Policy Update, Performance Management, January 2016)

Original Finding
The College website still holds the policy for Individual Staff Review and has not been updated for the new Staff Performance and Development Review. The Individual Staff Review policy was superseded by the new Staff Performance and Development Review in August 2015.

Original Recommendation
We recommend that the Staff Performance and Development Review policy is uploaded to the website and the redundant Individual Staff Review policy is removed.

Original Management Response
Agreed. Awaiting approval of Policy by JCC. Publication will follow immediately thereafter

Ref	Finding from our 2016/17 Follow Up	Grade	Recommendation
6	The Staff Performance and Development Review Policy is now available on the website.	Low	No further action required.

D GRADING STRUCTURE

For each area of review we assign a level of assurance in accordance with the following classification:

Assurance	Classification
Strong	Controls satisfactory, no major weaknesses found, no or only minor recommendations identified
Substantial	Controls largely satisfactory although some weaknesses identified, recommendations for improvement made
Weak	Controls unsatisfactory and major systems weaknesses identified that require to be addressed immediately
No	No or very limited controls in place leaving the system open to significant error or abuse, recommendations made require to be implemented immediately

D GRADING STRUCTURE

For each recommendation we make we assign a grading either as High, Medium or Low priority depending upon the degree of risk assessed as outlined below:

Grading	Classification
High	Major weakness that we consider needs to be brought to the attention of the Audit Committee and addressed by senior management of the College as a matter of urgency
Medium	Significant issue or weakness which should be addressed by the College as soon as possible
Low	Minor issue or weakness reported where management may wish to consider our recommendation

Audit Approach

Our approach to the review has been:

- Review outstanding recommendations and gain audit evidence to ensure that these have been addressed by the College.

Potential Key Risks

The potential key risks associated with the area under review are:

- The College does not address the areas of concern which may significantly affect its ability to continue to operate.