F

AUDIT COMMITTEE REPORT

Subject: Internal Audit Assignment – Follow Up Review	**Purpose:** **For Approval** ☒ **For Discussion** ☐ **For Information** ☐
Prepared by: Hazel Robertson, Vice Principal – Finance and Corporate Services	**Date:** 5 May 2020

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:

"We can conclude that the College have endeavoured to implement recommendations as far as possible with 4 of the 8 recommendations being fully implemented. In areas where recommendations have not been fully implemented, the College are still considering these in line with ongoing business and development".

Recommendation: Committee 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For publication ☒	**For publication with redactions** ☐	**Not for publication** ☐

Wylie+Bisset
Chartered Accountants, Business & Tax Advisers

Borders College

Internal Audit 2019/20

Follow Up Review

March 2020

Overall Conclusion
Substantial

TABLE OF CONTENTS

Section		Page
1.	Executive Summary	3
2.	Audit Arrangements	6
Appendices		
A.	Partially Implemented Recommendations	8
B.	Fully Implemented Recommendations	13
C.	Grading Structure	18
D.	Assignment Plan	20

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 2018/19 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 2019/20 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 have endeavoured to implement recommendations as far as possible with 4 of the 8 recommendation being fully implemented. 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 –Partially Implemented Recommendations	1	1	2	4
Appendix B – Fully Implemented Recommendations	1	2	1	4

Implementation of Recommendations

Summary of Implementation			
Audit Area	**Total**	**Partially Implemented**	**Fully Implemented**
Payroll	2	-	2
ICT	5	3	2
Follow Up	1	1	-
Total	**8**	**4**	**4**
Percentage of Total	**100%**	**50%**	**50%**

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	9 March 2020
Closing meeting	11 March 2020
Draft report issued	25 March 2020
Receipt of management responses	4 May 2020
Final report issued	5 May 2020
Audit Committee	21 May 2020
No of audit days	3

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
Senior Manager	Stephen Pringle	Senior Internal Manager	stephen.pringle@wyliebisset.com
Auditor	Faisal Kayani	Internal Audit Senior	faisal.kayani@wyliebisset.com
Auditor	Siobhan Archibald	Internal Auditor	Siobhan.Archibald@wyliebisset.com

Borders College			
Key Contact	Hazel Robertson	Vice Principle – Finance & Corporate Services	hrobertson@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

Partially Implemented Recommendations

Partially Implemented Recommendations

Data Leakage Prevention, IT Systems, April 2019

Original Finding
Data Leakage Prevention (DLP) is a strategy for making sure that end users do not send sensitive or critical information outside the corporate network. The term is also used to describe software products that help a network administrator control what data end users can transfer.

During our review, we found that the College did not have a DLP system in place and that removable media and access to cloud storage (eg DropBox, OneDrive) could be accessed as there are no restrictions in place to block them.

Original Recommendation
We recommend that the College puts stronger controls in place and looks at locking down all forms of removable, and cloud-based storage that is not required to be accessed. Controls could be put in place by utilising Group Policy to lock down removable media and web filtering software to block access to cloud storage systems.

We also recommend that the College look to monitor Office 365 for sensitive data across the Office 365 suite utilising the built-in technology that comes with Office 365.

We also recommend that the College investigate looking at software to monitor for Sensitive/Personal/confidential information for example Zonefox.

Ref	Finding from our 2019/20 Follow Up	Grade	Recommendation
1	This is partially implemented as the College is waiting until Microsoft Office 365 is live before they begin locking down other forms of media. As such, Office 365 will be available to staff from 13 March 2020. The College are allowing for a transitionary period of a couple of months before other media is locked down. This will involve the Head of IT informing staff to migrate all files over to Office 365. The SLT are yet to approve plans surrounding Office 365 implementation and the Head of IT is in the process of creating an action plan for stopping the usage of USBs.	High	We recommended that the College continue with their implementation of Office 365 and develop an action plan for locking down all other forms of media once the transitionary period is complete.

Management Response	Responsibility and Implementation Date
Office 365 email and OneDrive migration is currently underway which when complete will allow us to implement DLP strategy by restricting use of USB storage devices. Delay on this due to overrun of IDM and Office 365 project and resources due to Covid19 situation.	*Responsible Officer: Head of ISLT* *Implementation Date: August 2020*

Partially Implemented Recommendations

Patch Management, IT Systems, April 2019

Original Finding
Patches can be security fixes to fix vulnerabilities found within software. Patch Management is a strategy for managing patches or upgrades for software applications and technologies. A Patch Management Plan can help a business or organisation handle these changes efficiently.

During our review, we found that there is no set procedure to patch and test patches prior to deployment and when done this is on an inconsistent basis. We also found that Microsoft Products are patched utilising Microsoft System Centre Configuration Manager (SCCM) but that Third Party Applications (eg Jave, Adobe Reader, Adobe Flash) were not being updated.

Original Recommendation
We recommend that patching strategies are put in place to ensure that applications and operating systems are updated in a timely fashion when fixes are released.

We also recommend that the College investigate utilising SCCM to see if the software can patch the non-Microsoft Products. If this cannot be done then look for a third party solution to achieve this, for example PDQ Deploy, Chocolatey, BathPatch

Ref	Finding from our 2019/20 Follow Up	Grade	Recommendation
2	The Head of IT has developed a patching strategy where their Servers Patching Strategy is close to completion and their Network Infrastructure Patching Strategy is a working progress.	**Medium**	We recommend that the College complete patching strategies for Servers and Network Infrastructure.

Management Response	Responsibility and Implementation Date
Servers currently have a patching strategy in place which is a combination of automated patching for 'low risk' servers using SCCM whilst critical and high risk servers are a manual process. Both are completed on a monthly basis. We have implemented PDQ Deploy software to manage our 3rd party applications. Network Infrastructure schedule in progress and will be completed in June. Manual upgrades currently in place	*Responsible Officer: Head of ISLT* *Implementation Date: June 2020*

Partially Implemented Recommendations

IT Disaster Recovery Plan, IT Systems, April 2019

Original Finding
An IT Disaster Recovery Plan (DR Plan) can help to keep the IT Systems running in the event of a disaster. A plan sets out, but is not limited to, who does what and what happens in different scenarios. A Disaster Recovery Plan forms part of the Business Continuity Plan as this helps the IT Department know what systems must be brought back up first in the event of a disaster.

During our review with IT Staff, we found that the IT DR Plan was still in draft and had not been updated since changes were made to IT Systems within the College.

Original Recommendation
We recommend that the College update the plan and test to make sure that the IT Systems can be brought online in the event of a disaster.

Ref	Finding from our 2019/20 Follow Up	Grade	Recommendation
3	The College have updated their Disaster Recovery Plan, however, are yet to include processes for an event in which the whole IT System is brought down. The Head of IT has been in discussions with the Vice Principal to conduct testing over Summer 2020 and develop an appropriate plan to ensure that systems are prioritised appropriately.	Low	We recommend that the College complete the required tests over Summer 2020 and update their Disaster Recovery Plan accordingly.

Management Response	Responsibility and Implementation Date
Full system failure test was planned for Summer 2020, however due to the current Covid19 situation we have to revisit this once staff are back in the college.	*Responsible Officer: Head of ISLT* *Implementation Date: TBC*

Partially Implemented Recommendations

Financial Procedures Manual, Budgetary & Financial Controls, April 2018

Original Finding
During our review, we found that the Financial Procedures Manual was due to be reviewed in June 2017, however, this has yet to be completed. We note that the College's previous Head of Finance & Procurement had begun to review the document this has yet to be completed. We also note that the procedures within the manual are still relevant although there are areas that require updating such as job titles throughout the document.

Original Recommendation
We recommend that the College review and update the Financial Procedures Manual.

Finding on Follow Up 2018/19
The College has started to draft the updated Financial Procedures Manual and the Vice Principal: Finance & Corporate Services notes that a workshop on purchasing and procurement on this has been set up for May 2019.

Recommendation on Follow Up 2018/19
We recommend that the College continue to update the Financial Procedures Manual and hold the workshop as planned in May 2019.

Ref	Finding from our 2019/20 Follow Up	Grade	Recommendation
4	The College held their workshop in May 2019. However, the College has yet to update the Financial Procedures. This is due to a change in personnel. The College's Finance Business Partner joined in August 2019 and has been tasked with updating the Financial Procedures. This will begin following the update to the Colleges finance system due in March 2020.	Low	We recommend that following the update to the finance system, the College review and update their Finance Procedure Manual.

Management Response	Responsibility and Implementation Date
On completion of the SUN upgrade which is programmed for completion at the end of May 2020, the Finance Business Partner will undertake a systematic review of financial procedures. The intention is, the introduction of a Financial Procedures Manual, which is "future proof", easier to update for changes in processes, and more user "friendly" and has been the product of the current incumbents.	*Responsible Officer: Finance Business Partner* *Implementation Date: TBA*

Appendix B

Fully Implemented Recommendations

Fully Implemented Recommendations

Web Filtering, IT Systems, April 2019

Original Finding
A web filter is a program that can screen an incoming web page to determine whether some or all of it should not be displayed to the user. The filter checks the origin or content of the web page against a set of rules provided by a company or a person who has installed the web filter. They can also scan for malware on websites and block these as well.

During our review of the College's web filtering from Barracuda, we found that this was not functioning across all networks, eg EduRoam Wireless Network within the College and we were able to access inappropriate sites.

Original Recommendation
We recommend that the College implement a system that can protect all networks from accessing inappropriate websites and can protect against known bad websites and malware.

Ref	Finding from our 2019/20 Follow Up	Grade	Recommendation
1	The College has procured the services of 40 Net to provide a web filtering system on a 3-year contract.	High	No further action required.

Fully Implemented Recommendations

Digitalisation, Payroll, May 2019

Original Finding
A key part of the payroll process is the submission, review and authorisation of timesheets, which, in larger Colleges, is more commonly done online. This mitigates some of the risk of human error, and refines the process, allowing the staff more time for analysis.

During our review, we found that the College operates a largely paper based timesheet and expenses system. This occupies a great deal of the HR Officer's time ensuring all of the documents have been authorised by the relevant staff member.

Original Recommendation
We recommend that the College considers the possibility of implementing a digital timesheet processing system.

Ref	Finding from our 2019/20 Follow Up	Grade	Recommendation
2	The College has developed an Implementation Plan for adopting a Digital Timesheet Processing System. The College aim to have this fully implemented by April 2020.	Medium	No further action required.

Fully Implemented Recommendations

Disaster Recovery Testing, IT Systems, April 2019

Original Finding
A Disaster Recovery Test (DRT) is carried out to ensure that restores of systems are tested, so that in event of a disaster there is faith in the processes being used to recover the systems. Any issues should then feed back into IT DR Plan.

During our review, we found that tests were being completed but not on a formal process where outcomes are documented.

Original Recommendation
We recommend that the College implement a disaster recovery testing process and all testing is documented. Any issues found that would affect the IT DR Plan should feedback into the IT DR Plan.

Ref	Finding from our 2019/20 Follow Up	Grade	Recommendation
3	The College has completed disaster recovery testing and all testing is documented.	Medium	No further action required.

Fully Implemented Recommendations

Overpayments Procedure, Payroll, May 2019

Original Finding
Overpayments are not a common occurrence within the College, however, they are often identified during month on month checks carried out by the HR Officer.

Despite the payroll staff dealing with overpayments in an appropriate manner, the procedure is not specifically documented within the manual.

Original Recommendation
We recommend that the Payroll Manual be updated with a procedure note for the overpayments process.

Ref	Finding from our 2019/20 Follow Up	Grade	Recommendation
4	The College has now updated their Payroll Manual to include a procedure note for overpayments.	Low	No further action required.

C 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

C 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 will be:

- 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.