B

AUDIT COMMITTEE

BORDERS COLLEGE REGIONAL BOARD

Subject: Internal Audit Assignment – Disaster Recovery	**Purpose:** **For Approval** ☒ **For Discussion** ☐ **For Information** ☐
Prepared by: Kirsty Robb – VP Finance and Corporate Services	**Date of Committee:** 5 October 203

Purpose: To present to the Committee the findings of the Disaster Recovery audit undertaken by Wylie Bisset, the Colleges Internal Auditors.

Executive Summary:
The audit of Disaster Recovery Testing forms part of the approved internal audit plan for 2022/23.

The Auditors report states "Following our review, we can provide a strong level of assurance that the College's Disaster Recovery testing process is robust and that any lessons learned during this process are fully implemented"

The report did not identify any recommendations but did highlight 5 areas of good practice

Key items:
The full report is attached in appendix A.

Questions that Members should ask themselves when reading the paper:
Is the Committee content with the findings of the report?

Linked to Strategic Ambition(s):
Create high quality learning and training opportunities which are relevant, enabling and flexible
Take a leading role in enabling an inclusive, resilient and sustainable Scotland

Performance Measures:
Student, staff & employer satisfaction in top quartile nationally
Recognised as national leaders in sustainable practice

Linked to Strategic Risk Register:
4b - Governance
Choose an item.

Recommendation: The Committee approve the contents of the report

Previous Committee Approvals:

For publication ☒	**Not for publication** ☐ **If not, why not?**

Wylie + Bisset
Accountants, Business & Tax Advisers

Borders College
Internal Audit 2022-23

Disaster Recovery Testing
May 2023

Overall Conclusion
Strong

TABLE OF CONTENTS

Section **Page**

1 EXECUTIVE SUMMARY 2
2 BENCHMARKING 8
3 AUDIT ARRANGEMENTS 9
4 KEY PERSONNEL 10

Appendix **Page**

A GRADING STRUCTURE 12
B ASSIGNMENT PLAN 14

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. Every sound system 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

Overview

Purpose of review

The purpose of this assignment was to review and assess the process and results of the College's Disaster Recovery testing to ensure that this was robust and that any lessons learned from the testing were implemented. We also reviewed the training arrangements in place at the College.

This review forms part of our 2022/23 Internal Audit Annual Plan.

Scope of review

Our objectives for this review were to ensure:

- The College undertake regular Disaster Recovery testing.
- The testing completed is robust and fully considers the effects that this will have on the College.
- The College reviews and considers the outcome of Disaster Recovery tests.
- The College has a robust training programme in place for relevant staff members throughout the College.

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

Limitation of scope

There is no limitation of scope.

1 EXECUTIVE SUMMARY

Background

The IT Team

The College's IT systems are supported by their own, internal IT Team. They are responsible for ensuring hardware is configured for staff, software is kept up to date, and data is backed up appropriately. In partnership with the College's Internet Service Provider, Jisc Services Limited, they ensure that the College's internet provision is appropriately monitored. The IT Team are responsible for overseeing the network and ensuring all devices are protected by robust anti-virus/anti-malware solutions.

Disaster Recovery

The College has made a significant move by locating their production network to a customised data centre facility maintained by DataVita, the cloud and data centre service provider. This 'infrastructure as a service' (IaaS) offering allows the College to leverage the multiple layers of security offered by this resilient and reliable bespoke environment. Not only does this facility offer peace-of-mind in terms of physical security for the business-critical equipment, but it also provides robust support systems for power, bandwidth, cooling, and redundancy within a single plan.

Transitioning from managing data in-house to outsourcing within a data centre has helped the College to design a robust Disaster Recovery solution. The 'Disaster Recovery as a service' (DRaaS) offering from DataVita would allow the College to failover onto a secondary data centre location should the network services housed within the primary data centre be rendered inaccessible.

Backup Solution

In terms of their backup provision, the College again use the services of DataVita who provide a 'backup as a service' (BaaS) offering to protect the servers and services located within their Data Centre.

Backups are taken incrementally. After the initial backup seed, all subsequent backups are snapshots of the changed blocks from the period between the previous backup and when the next backup is taken. All backups can be recovered as if they were 'full' backups within the set Retention Policy.

Disaster Recovery/Business Continuity targets a recovery point objective of 1 hour, with a recovery time objective of 2 hours. As the servers are remote there is no requirement for any on-site backup appliance.

1 EXECUTIVE SUMMARY

Work Undertaken

Our work for this review included the following:

Objective 1: The College undertake regular Disaster Recovery testing.

- We held discussions with the College to establish the current arrangements in place.
- We reviewed the College's testing procedures and whether these were being scheduled appropriately.

Objective 2: The testing completed is robust and fully considers the effects that this will have on the College.

- A review of the scope of the testing that takes place.
- A review of the scheduling of the tests and whether these are timetabled to avoid potential user disruption.

Objective 3: The College reviews and considers the outcome of Disaster Recovery tests.

- A review of the College's response to any potential anomalies or failures that occur during the testing process.

Objective 4: The College has a robust training programme in place for relevant staff members throughout the College.

- A review of the training that the IT Team have undergone to help consolidate their understanding of the College's Disaster Recovery provision.
- A review of the understanding the IT Team have of their roles in the event that the Disaster Recovery process is invoked.

1 EXECUTIVE SUMMARY

Conclusion

Overall conclusion

Overall Conclusion: Strong
Following our review, we can provide a strong level of assurance that the College's Disaster Recovery testing process is robust and that any lessons learned during this process are fully implemented.

Summary of recommendations

Grading of recommendations				
	High	Medium	Low	Total
Disaster Recovery Testing	0	0	0	0

As can be seen from the above table there were no recommendations made.

1 EXECUTIVE SUMMARY

Areas of good practice

The following is a list of areas where the College is operating effectively and following good practice.	
1.	The College test the Disaster Recovery provision annually, as part of DataVita's DRaaS offering. The test simulates the catastrophic failure of the primary infrastructure, allowing the IT Team to measure the success of the network services 'failing over' onto the secondary site in Edinburgh. This test must match the requirements of the Service Level Agreement (SLA) in place for 'Restore Time Objectives' (RTO) and 'Restore Point Objectives' (RPO) in a disaster scenario.
2.	Although the College's Disaster Recovery and Backup provision is maintained by DataVita, the IT Team have been trained on their roles and understand their responsibilities in the event of a disaster scenario affecting IT. Should Disaster Recovery be invoked, the Director of IT & Digital will lead a team who are responsible for the support of the restoration of key IT services. In consultation with DataVita this team are tasked with ensuring the smooth transition onto the secondary Data Centre facility, with minimal impact to network users.
3.	The IT Team take appropriate action to rectify any issues that are identified following the completion of a scheduled Disaster Recovery test. Problems are appropriately recorded, with the affected instances tested again until the IT Team are fully satisfied that all operations have been completed.
4.	The critical IT equipment that makes up the College network is housed in a Tier 3 Data Centre, which has redundant and dual-powered servers, storage, network links and other IT components. These IT components are powered with multiple, active, and independent sources of power and cooling resources. All of these security and environmental services are monitored by DataVita, and any alerts are acted upon by their internal support team.

1 EXECUTIVE SUMMARY

The following is a list of areas where the College is operating effectively and following good practice.	
5.	The College has a robust Backup and Disaster Recovery Plan in place. Having migrated their servers into a Data Centre facility, the College has invested in DRaaS and BaaS which is wholly managed by their partner DataVita. The detail around the solution is documented, including the SLA for the RTO and RPO of all digital services in the event of a catastrophic failure of the primary site.

2 BENCHMARKING

We include for your reference comparative benchmarking data of the number and ranking of recommendations made for audits of a similar nature in the most recently finished internal audit year.

Disaster Recovery Testing

Benchmarking				
	High	Medium	Low	Total
Average number of recommendations in similar audits	1	1	1	3
Number of recommendations at Borders College	0	0	0	0

From the table above it can be seen that the College has a lower number of recommendations compared to those colleges it has been benchmarked against.

3 AUDIT ARRANGEMENTS

The table below details the actual dates for our fieldwork and the reporting on the audit area under review. The timescales set out below will enable us to present our final report at the next Audit Committee meeting.

Audit stage	Date
Fieldwork start	26 April 2023
Closing meeting	3 May 2023
Draft report issued	11 May 2023
Receipt of management responses	3 July 2023
Final report issued	5 July 2023
Audit Committee	5 October 2023
Number of audit days	3

4 KEY PERSONNEL

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

Wylie & Bisset LLP			
Partner	Graham Gillespie	Partner	graham.gillespie@wyliebisset.com
Senior Internal Audit Manager	Sue Brook	Senior Internal Audit Manager	susan.brook@wyliebisset.com
Senior	Kevin McDermott	Senior IT Auditor	kevin.mcdermott@wyliebisset.com

Borders College			
Key Contact	Scott Moncreiff	Director of IT & Digital	smoncrieff@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.			

APPENDICES

A 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.

A GRADING STRUCTURE

For each recommendation, we assign a grading either as High, Medium, or Low priority depending on 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.

B ASSIGNMENT PLAN

Purpose of review

The purpose of this assignment is to review and assess the process and results of the College's Disaster Recovery testing to ensure that this is robust, and any lessons learned from the testing are implemented. We will also review the training arrangements in place the College.

This review forms part of our 2022/23 Internal Audit Annual Plan.

Scope of review

Our objectives for this review are to ensure:

- The College undertake regular Disaster Recovery testing.
- The testing completed is robust and fully considers the effects that this will have on the College.
- The College appropriate review and consider the outcome of the Disaster Recovery test.
- The College has robust training programme in place for relevant staff members throughout the College.

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

Limitation of scope

There is no limitation of scope.

Audit approach

Our approach to the review will be:

- Discussion with staff involved to establish the current arrangements in place at the College for Disaster Recovery.
- Review of Disaster Recovery planning, documentation, and processes.
- Review of support and maintenance for business critical services.
- Review of environment for business critical services.
- Review of Disaster Recovery training arrangements.
- Review the College's processes for evaluating the outcomes of Disaster Recovery testing.

Potential key risks

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

- There is no Disaster Recovery plan and Business Continuity procedures and plans in place.
- IT systems are located in insecure or inadequate environments.
- There is no formal testing being carried out for Disaster Recovery and Business Continuity procedures.
- No training has been provided for Disaster Recovery and Business Continuity procedures.