Wylie Bisset
Accountants, Business & Tax Advisers

UHI North, West and Hebrides
Internal Audit 2023-24

IT Systems Integration
March 2024

Overall Conclusion
Substantial

TABLE OF CONTENTS

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 UHI North, West and Hebrides'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.

Wylie + Bisset

1 EXECUTIVE SUMMARY

Overview

Purpose of review

The College has recently merged from three colleges to one. This resulted in IT systems being integrated. The purpose of this assignment was to review the IT systems in place for the merged College and to provide assurance on its adequacy for the College.

This review forms part of our 2023/24 Internal Audit Annual Plan.

Scope of review

Our objectives for this review were to ensure:

- There were appropriate policies in place to provide governance and control over the College's IT systems.
- There were appropriate solutions in place to control access to the College's information systems.
- There were appropriate solutions in place to aid in securing the College's IT network which are being monitored effectively.
- There were appropriate Disaster Recovery and Business Continuity plans in place for the College's IT systems that were being tested.
- The current IT arrangements met the business needs of the College and represented value for money.
- There was assurance that all relevant data had migrated over correctly to the integrated IT System.

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 was no limitation of scope.

1 EXECUTIVE SUMMARY

Background

College Merger

UHI North, West & Hebrides is a constituent College of the University of the Highlands and Islands (UHI). It operates through a network of learning centres and offers distance learning options. The College serves rural and island communities across the North, West, and Outer Hebrides.

UHI North, West & Hebrides was formed through the merger of three Colleges:

- UHI North Highland;
- UHI Outer Hebrides; and
- UHI West Highland.

On August 1, 2023, UHI North, West & Hebrides officially came into existence with launch activities taking place in September of that year. The merger aimed to enhance educational opportunities and strengthen the collective impact of these colleges across the North, West, and Outer Hebrides regions of Scotland.

IT Team

The discreet IT Teams at each of the three Colleges were merged into a single team under the leadership of the ICT Services Manager. Whilst continuing to offer a local presence at each site, the collective IT Team now have a shared responsibility for ensuring hardware is configured for staff, software is kept up to date, and all relevant devices are protected by robust anti-virus/anti-malware solutions. In conjunction with colleagues from the UHI Learning and Information Services Team (LIS), they ensure that College data and associated software and services are backed-up and secure. Similarly, in partnership with the College's Internet Service Provider, Jisc Services Limited, they ensure that the College's internet provision is monitored should there be an attempted security breach or equipment failure.

Service Consolidation & IT Integration

Prior to the merger, UHI already had a single Microsoft 365 (M365) tenancy that delivered cloud services specific to the three merging Colleges, e.g., OneDrive, SharePoint etc. Therefore, during the merger process, there was no significant requirement for the College to concern themselves with systems integration in terms of Microsoft's software and services. Post merger, the College business units, such as Payroll &

Finance, did have to standardise on applications that would be used across the three sites e.g. Infor SunSystems would become the accounting software to be used by all relevant staff at the College. However, a significant effort was already underway at UHI to migrate as much data, software, and services onto cloud platforms as possible. As a consequence, server numbers had reduced significantly with remaining servers migrated away from their previous local role and into secure data centre facilities supported and managed by the ILS Team.

It is clear that the previous and continued good practice around design and consolidation helped mitigate potential issues relating to data loss, corruption, or degradation during the merger process. The IT Team's careful planning, execution, and ongoing evaluation post-merger has helped to maintain the data integrity and functionality of the integrated IT systems.

Efficiencies & Improvements

During our review, we were pleased to observe the obvious efficiencies in place at the College. We commend the College for having achieved Cyber Essentials Plus accreditation. The accreditation cannot be achieved without the College network being built upon modern, supported Windows Operating Systems that are robustly secured and configured. Additionally, we recognise the significant efforts that have been made by the College to ensure that post-merger software licence purchases leverage savings through site-wide licencing agreements. New licencing models have now been agreed to reflect that the College is now a single educational establishment instead of three separate entities. This level of due diligence, facilitated by the IT Team, the College Procurement Team and with input from relevant stakeholders, has realised immediate cost saving benefits for the College.

For all of the good practice that is clearly in place at the College, we have recommended that the IT Team schedule regular testing of the robust Disaster Recovery and backup provision that is in place to protect their remaining servers. We acknowledge that the software used will alert the Learning and Information Services (LIS) Team should there be a backup failure and that restores of critical system backups do take place. However, we believe the IT Team should look to schedule test scenarios, perhaps creating checklists to record the success or otherwise of each process they choose to evaluate. We have raised a recommendation in respect of this, please see **Section 3: Detailed Recommendations** for further information.

1 EXECUTIVE SUMMARY

Work Undertaken

Our work for this review included the following:

Objective 1: There are appropriate policies in place to provide governance and control over the College's IT systems.

- We held discussions with the College to establish the current arrangements in place.
- We reviewed the College's policies and procedures to assess whether these are robust and in line with best practice.

Objective 2: There are appropriate solutions in place to control access to the College's information systems.

- A review of IT security, access control and user policies for adequacy. **Please see Section 3: Detailed Recommendations for further information.**
- A review of the College's anti-virus/ anti-malware software including web protection.
- A review of the College's data leakage prevention controls and monitoring. **Please see Section 3: Detailed Recommendations for further information.**

Objective 3: There are appropriate solutions in place to aid in securing the College's IT network which are being monitored effectively.

- A review of the College's network security appliances and monitoring.
- A review of the College's network access controls including user account controls, remote access, and third-party access.

Objective 4: There are appropriate Disaster Recovery and Business Continuity plans in place for the College's IT systems that are being tested.

- A review of the College's IT Disaster Recovery and Business Continuity planning including the College's backup strategy. **Please see Section 3: Detailed Recommendations for further information.**

Objective 5: The current IT arrangements meet the business needs of the College and represent value for money.

- We held discussions with relevant stakeholders in order to assess the IT solutions in place and whether they met the needs of the College.
- We reviewed the process by which the College ensure they receive the optimum educational discounts when sourcing any new IT solutions or licence renewals.

Objective 6: There is assurance that all relevant data has migrated over correctly to the integrated IT system.

- We reviewed the College's IT architecture and data management solutions to ensure that there was an aligned process when in place for data migration.
- We held discussions with relevant stakeholders in order to assess their satisfaction that data had been migrated efficiently and effectively.

1 EXECUTIVE SUMMARY

Conclusion

Overall Conclusion: Substantial
We can provide a substantial level of assurance over the College's IT Systems Integration and the associated policies, procedures, and controls. Although we have raised several good practice points, we have made 2 medium grade recommendations and 1 low grade recommendation for improvement. We have also raised 1 observation for consideration. **Please see Section 3: Detailed Recommendations for further information.**

Summary of recommendations

Grading of recommendations				
	High	Medium	Low	Total
IT Systems Integration	0	2	1	3

As can be seen from the above table there were no recommendations made which we have given a grading of high.

Areas of good practice

The following is a list of areas where the College is operating effectively and following good practice.	
1.	There are robust procedures in place to ensure that the College receive value for money for the software licences they hold and utilise. This includes using Jisc Chest, the not-for-profit membership organisation that negotiates preferential licence agreements for software and online resources delivered to the academic sector. Similarly, the software present on the College network has clearly been put in place with staff and student experience in mind. Close co-operation between the College IT Team, the Procurement Team, academic departments, and College business units help ensure that the user experience is as positive as possible with the most cost-effective licencing model available.
2.	The IT Team are responsible for ensuring that robust backup and Disaster Recovery procedures are in place to protect the College's network services and systems. The College replicate their virtual servers onto a secondary network facility located on the Inverness College campus. Should the College suffer a loss to the live network, they have the ability to 'failover' onto the secondary network with minimal user disruption. The efficacy of this process is monitored and verified by the backup & recovery software.
3.	The College has appropriate documentation detailing the Disaster Recovery arrangements in place to restore the IT network in the event of a disaster scenario. There is a formal, approved Business Continuity Plan and IT Disaster Recovery Plan that detail the arrangements to mitigate the impact of such an event. The roles and responsibilities of key staff are described within the documents.
4.	The College has suitable anti-virus and anti-malware security in place across all endpoint devices. The College have email security via their Microsoft Defender 365 solution, which scans all email and file attachments for activity such as phishing and malware.

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 patching regime in place, with servers and endpoint devices patched on a regular basis and scheduled appropriately. Microsoft Intune is used to install and monitor the endpoint updates. Should Microsoft advise that a patch be applied immediately to guard against a known vulnerability, then the IT Team will prioritise accordingly.
6.	The College has achieved Cyber Essentials Plus accreditation and as part of the award must submit to an annual internal and external vulnerability scan of the network, conducted by the awarding body. The IT Team then look to address any of the issues that may be highlighted.
7.	There are appropriate change management procedures in place at the College. The IT Team test and document all network changes, using tickets on their service desk, to ensure there is a point of reference in the event of any issues or security incidents that occur as a result. All user level changes are recorded by the IT Team, as well as recording issues resolved. All major changes to the IT network require consultation with the Change Approval Board before being implemented across the College network.
8.	The College has robust logging, monitoring, and alerting arrangements in place. This includes the functionality offered by SolarWinds Orion, the network server and IT infrastructure monitoring software. It provides holistic network visibility of all relevant systems, services, and applications on the network. Similarly, the Microsoft Defender anti-virus solution will alert upon and protect the College against unusual endpoint activity and targeted attacks.

1 EXECUTIVE SUMMARY

The following is a list of areas where the College is operating effectively and following good practice.	
9.	The College has robust processes in place when required to create or disable staff accounts. If a member of staff is starting or leaving the College, HR personnel will contact the IT Team. For those starting employment with the College, the IT Team will create a user profile, supplying them with access to the requisite applications and adding appropriate network privileges. For leavers, user access is removed immediately or on the date communicated. Licences can then be cancelled, and the information logged and set as completed. Third Party access to the IT network is achieved when the IT Team facilitates a secure remote session for the named organisation, with network privileges granted only by the IT Team and the session shadowed appropriately.
10.	The College has robust physical and environmental controls protecting its core network equipment. The equipment is secured in locked rooms with air conditioning and flame suppressing equipment. The doors to the server rooms and cabinets are secured by default, with access available only to the IT Team alongside relevant College staff.
11.	For staff accessing College resources remotely, access is restricted to the cloud-based software and services available through Microsoft 365. Permissions are strictly controlled, with access to all resources requiring Active Directory credentials and additional security enforced through Multi-Factor Authentication (MFA). College supplied Windows mobile devices are further protected through the use of the encryption software, BitLocker.
12.	Wireless access is appropriately separated for different users on the network. Access is segregated using Service Set Identifiers (SSID's), with unmanaged devices restricted to external resources only i.e., hosted on the Internet. Access to College network resources is secured using domain credentials for both staff and students. Security is again enhanced by internet filtering and security rules set on the College firewall. Further external protection is provided by the College's Internet Service Provider, Jisc Services Limited.

1 EXECUTIVE SUMMARY

The following is a list of areas where the College is operating effectively and following good practice.	
13.	The College has robust policies and procedures in place to provide governance and control over IT systems. These include, but are not limited to, the following: ➢ Hybrid Working Policy; ➢ Acceptable Use Policy; ➢ Data Protection Policy; ➢ Bring Your Own Device Policy; ➢ Computer Operations Policy; ➢ Incident Management Policy; ➢ Password Control Policy; ➢ Protection Against Malicious Software Policy; ➢ Responsibilities of Users With Elevated Rights Guide; ➢ Third Party Access Policy; and ➢ Vulnerability Testing Procedures. These policies and procedures are regularly updated.
14.	The task to ensure that all relevant data could migrate seamlessly onto the College's integrated IT System was set in motion well before the official 2023 merger. The creation of a single M365 tenancy for the College, designed in advance of the merger, allowed users to access relevant digital resources before and after the official date. Additionally, the consolidation of servers, with many digital services now delivered via SaaS (Software as a Service), has allowed the College to avoid simple data storage dumps. Instead of transferring all data blindly, the College has focussed on migrating data that is both relevant and necessary.

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.

IT Systems Integration

Benchmarking				
	High	Medium	Low	Total
Average number of recommendations in similar audits	0	2	1	3
Number of recommendations at UHI North, West and Hebrides	0	2	1	3

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

3 DETAILED RECOMMENDATIONS

Engagement and Training			
Ref.	Finding and Risk	Grade	Recommendation
1.	As part of any organisation's cyber security approach, staff training has become an increasingly vital component. Mandatory and regular cyber security training can empower users to take control of their own ability to avoid cyber security malpractice. During our review, we found that the College had no mandated cyber security training in place for new staff and no regular, refresher cyber security training for existing staff. Whilst we note that the College conduct annual phishing exercises and that staff must complete training modules relating to data and computer security, there is no formal cyber training in place. There is an ever-increasing risk of attackers exploiting human nature with diversionary tactics, such as creating a false sense of urgency or impersonating trusted people. The risk of not investing in cyber security training for staff is that it could leave your frontline defence unprepared and	**Medium**	We recommend that the College take appropriate steps to ensure that mandatory cyber security training is embedded in the induction programme for all new staff. A formal programme of refresher training should then be established for all staff with a risk-based approach adopted in identifying the frequency of refresher training requirements. Appropriate training will help empower staff with the knowledge and skills to recognise cyber threats and from there be able to make informed decisions.

	exposed against such cyber-attacks.		
Management response			Responsibility and implementation date
Information security, Computer Security, and Password security modules already in play, just nothing under the single header of “Cyber security” – nonetheless discussions with Compliance Manager resulted in a new set of modules from our training supplier, which on testing fit the bill very nicely. Note that the modules offered by the supplier still don’t come with the name “Cyber Security” but are their recommendation to meet that requirement, and has been verified to be appropriate by ICT Manager.			*Responsible Officer: Compliance Manager* *Implementation Date: 31 October 2024*

3 DETAILED RECOMMENDATIONS

Disaster Recovery Testing Procedures			
Ref.	Finding and Risk	Grade	Recommendation
2.	Disaster Recovery testing is undertaken to ensure that the Disaster Recovery and/or Business Continuity Plan is robust and that it is sufficient to address any disaster affecting the system. We acknowledge that the backups and replications protecting College systems are robust and appropriately monitored. The backup software will report on the efficacy of the backups themselves and alert upon any potential issues. We also acknowledge that the IT Team have previously practiced their response to a disaster scenario, enacting various activities to test staff preparedness for such an event. However, the IT Team should look to schedule formal Disaster Recovery Testing in order to confirm that the College would recover fully following a disaster scenario, with the details of the tests themselves appropriately documented. There is the risk that the lack of a thoroughly tested procedure to address a disaster scenario could impact upon the timely and appropriate response	**Medium**	We recommend that the College schedule a regular test of the current backup and Disaster Recovery solution, and that the steps are formalised, and the findings documented. These tests would involve, but may not be limited to: ➢ A formal test to ensure that the solutions in place are robust and working properly. ➢ Benchmarking to ensure the expected downtime and expected recovery time of these business-critical solutions match the College's assumptions around Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO). ➢ A formal schedule to ensure that these tests are undertaken with appropriate frequency.

	of the IT Team to any catastrophic incident affecting IT.		
Management response			Responsibility and implementation date
Plan raised to implement bi-annual DRP test/drills in collaboration with UHI ITDI.			*Responsible Officer: ICT Manager* *Implementation Date: 10 February 2025*

3 DETAILED RECOMMENDATIONS

Data Leakage Prevention Risks			
Ref.	Finding and Risk	Grade	Recommendation
3.	DLP (Data Leakage Prevention) 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. We acknowledge that technical controls are in place to mitigate the risk of data being removed from the network via unmanaged USB storage devices. Data can only be written to encrypted USB devices. However, we found that technical settings to control access to unmanaged file sharing websites were not enforced. Data could be removed from the network by members of staff via unmanaged file sharing websites. This could result in a General Data Protection Regulation breach, with the risk of associated fines and/or damage to the College's reputation.	**Low**	We recommend that a risk assessment which considers DLP is conducted to ensure that any areas of risk, such as the use of unmanaged USB storage devices and access to unmanaged file-sharing websites, are assessed and that subsequent solutions are considered. The IT Team may then be tasked with providing additional security controls to mitigate these risks, helping the College to reduce the likelihood of deliberate or accidental data leakage.

Management response	Responsibility and implementation date
DPO to produce risk assessment in conjunction with ICT Team	*Responsible Officer: Data Protection Officer* *Implementation Date: August 2024*

4 OBSERVATIONS

The following is a list of observations from our review	
1.	During this review, and having spoken to a number of digital stakeholders, it was clear that the College had addressed and overcame many of the IT related challenges that they would face in the pre and post-merger period. However, we were made aware that students attending the College's Cyber Security classes do not have access to a sandboxed area in which they can safely test files, evaluate code, validate software, and detect malicious behaviour. A sandbox is a secure environment detached from the College's main system. It allows potentially harmful IT behaviour to be tested without posing a threat to the live network or critical systems. With so much positive feedback directed towards the IT Team and their delivery of related software and services, we would urge the team to investigate a solution that would deliver this controlled testing tool and enhance the delivery of this area of the curriculum to the students involved.

5 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 & Risk Management Committee meeting.

Audit stage	Date
Fieldwork start	11 March 2024
Closing meeting	18 March 2024
Draft report issued	26 March 2024
Receipt of management responses	1 May 2024
Final report issued	7 May 2024
Audit & Risk Management Committee	22 May 2024
Number of audit days	6

6 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 Manager	Sue Brook	Senior Internal Audit Manager	susan.brook@wyliebisset.com
Auditor	Kevin McDermott	Senior IT Auditor	kevin.mcdermott@wyliebisset.com
Auditor	Insert(GetColumn("Name"))<i>Shaun Roddan	IT Auditor	shaun.roddan@wyliebisset.com

UHI North, West and Hebrides			
Key Contact	Roddy MacPhee	Finance Manager	roddy.macphee@uhi.ac.uk
	Kate Hannay	ICT Services Manager	kate.hannay@uhi.ac.uk
	Graham Florence	ICT Team Leader	graham.florence@uhi.ac.uk
	Shona Thumpston	Payroll & Finance Officer	shona.thumpston@uhi.ac.uk
	Sarah Bruce	Curriculum Area Lead for Business Admin, Hospitality, Creatives Arts and Computing	sarah.bruce@uhi.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 & Risk Management 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.

Purpose of review

The College has recently merged from three colleges to one. This resulted in IT systems being integrated. The purpose of this assignment is to review the IT systems in place for the merged College and to provide assurance on its adequacy for the College.

This review forms part of our 2023/24 Internal Audit Annual Plan.

Scope of review

Our objectives for this review are to ensure:

- There are appropriate policies in place to provide governance and control over the College's IT systems.
- There are appropriate solutions in place to control access to the College's information systems.
- There are appropriate solutions in place to aid in securing the College's IT network which are being monitored effectively.
- There are appropriate Disaster Recovery and Business Continuity plans in place for the College's IT systems that are being tested.
- The current IT arrangements meet the business needs of the College and represent value for money.
- There is assurance that all relevant data has migrated over correctly to the integrated IT System

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 relevant staff involved to establish the current arrangements in place.
- Review of IT security, access control and user policies for adequacy.
- Review of the College's strategy for identifying and addressing system vulnerabilities and a secure and timely manner.
- Review of the College's anti-malware/virus software including web protection.
- Review of the College's network security appliances and monitoring.
- Review of the College's data leakage prevention controls and monitoring.
- Review of the College's network access controls including user account controls, remote access, third party access
- Review of the College's IT disaster recovery and business continuity planning including the College's backup strategy.
- Review of the College's IT equipment to ensure suitability.
- Review of the service received from the College's IT providers to ensure this is appropriate.
- Review of the College's IT strategy and reporting mechanisms.
- Sample testing of controls where applicable.

Potential key risks

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

- There are no/inadequate policies in place to provide governance and control over the College's IT systems.
- There is a lack of/inadequate controls in place to control access to the College's information systems.
- Security solutions in place to protect the College are ineffective and/or not being monitored appropriately.
- Disaster Recovery and Business Continuity procedures are ineffective, un-tested and not in line with the College's Business Impact Analysis.
- The current IT arrangements do not meet the business needs of the College and do not represent value for money.
- Inaccurate data has been transferred into the new integrated IT System.