(Paper 1A)

BOARD OF MANAGEMENT
ACTION TRACKER

COMMITTEE: **Audit Committee**

DATE RAISED	ACTION No	ACTION	DUE DATE	OWNER	STATUS*	COMMENTS
19.09.17	1	Consideration of cross representation between Audit Committee and BRIC	June 2018	A Walker	In progress	Matter raised with Board Chair at Board Meeting on 28 September 2017. Recommendation to the Board Meeting on 21.06.18 within the Review of the Revised Committee Structure Paper.
05.12.17	2	Raise with SFC the Committee's concerns over the SFC instructed rebadging of Net Depreciation in the 2016/17 Financial Statements as "Cash Budget for Government Directed Priorities"	March 2018	A Walker	Complete	Raised with the Interim CEO of the Scottish Funding Council at the Board Strategy Day on 20 February 2018.
20.03.18	3	Progress report on the on the work being undertaken by the College in response to the recommendations contained in the internal audit report on Business Continuity Planning	September 2018	M Breen	In progress	

SCHEDULE OF BOARD AND COMMITTEE MEETINGS 2017-2018

20.03.18	4	The Committee to monitor and receive progress reports on the cascading of operational risk registers down through the management structure of the College	September 2018	M Breen	Not started yet	
18.09.18	5	The receipt, consideration and approval of the Ayrshire College Business Continuity Plan to be an annual requirement of Committee business at the first meeting of each session.	September 2019	Responsible EMT Member	Completed for 2018-19. Rolling thereafter	
18.09.18	6	Discuss with Chair of LTC ownership of the Student Curriculum/Experience Review	June 2019	Chair of Audit	In progress	
18.09.18	7	Risk Register: BOM4 – Include PFI mitigation actions as included in the Financial Sustainability Plan. BRIC 7 – Be enhanced to 20 as recommended by BRIC	September 2018	M Breen	Completed	
27.11.18	8	Risk Register: BRIC7 Chair of Audit to discuss The proposed decrease in risk level with the Chair of BRIC following agreement of a timeline for the appointment of a	December 2018	Chair of Audit		

BOARD OF MANAGEMENT
ACTION TRACKER

		new Principal and a new Vice Principal,				

* ***Not Started / In Progress / Completed***

AYRSHIRE COLLEGE

INTERNAL AUDIT REPORT – DRAFT

RISK MANAGEMENT
JANUARY 2019

LEVEL OF ASSURANCE	
Design	Operational Effectiveness
Substantial	Substantial

DISTRIBUTION	
Brad Johnstone	Head of ICT
James Thomson	Director of Finance and Student Funding
Audit Committee	Members

REPORT STATUS LIST	
Auditors:	Scott Peterson
Dates work performed:	22 October - 26 October 2018
Draft report issued:	12 November 2018
Final report issued:	30 November 2018

EXECUTIVE SUMMARY

LEVEL OF ASSURANCE: (SEE APPENDIX I FOR DEFINITIONS)

Design		There is a sound system of internal control designed to achieve system objectives.
Effectiveness		The controls that are in place are being consistently applied.

SUMMARY OF RECOMMENDATIONS: (SEE APPENDIX I)

High		0
Medium		0
Low		1

TOTAL NUMBER OF RECOMMENDATIONS: 1

BACKGROUND:

As part of the 2018 - 2019 Internal Audit Plan, it was agreed that internal audit would review the risk management framework in place within Ayrshire College and compare this with good practice. The purpose of this review is to provide the Audit Committee with a level of assurance around the current arrangements, and to provide the Executive Management Team ("Management") with advice and recommendations for improving the arrangements further. The deliverables include this internal audit report and a populated risk management maturity model, to demonstrate to Management in detail the maturity status and actions which can be taken to further develop the risk management processes.

Ayrshire College first adopted a Risk Management Policy in May 2015. It has been reviewed and updated in 2015, 2017, and again in September 2018. The current version was approved in October 2018 by the Board of Management ("Board"). The Vice Principal, Finance & Skills is responsible for the Policy and the next planned review is August 2020. The Policy indicates 6 key principles:

1. The Board is responsible for overseeing risk management;
2. The Audit Committee is responsible with reviewing, discussing and approving the Risk Register at each Committee meeting;
3. The Risk Register must be updated quarterly prior to presentation to the Committees;
4. The Board and its Committees must adopt an open and receptive approach to solving risk problems;
5. Management must adopt a conservative and prudent approach for recognising and disclosing all risks and their implications;
6. All Management is responsible for encouraging good risk management practice within their areas of responsibility.

The College's Board sets the tone, the risk appetite, and influences the culture of risk management. It approves major decisions affecting the risk profile or exposure. Management implements risk management and internal control processes. The Board or its sub-committees agree on any new, emerging or changing risks at each of their regular meetings. Management reviews the register formally each quarter prior to reviewing with the Committees. Management is also responsible for identifying, evaluating and outlining the significant risks faced by the College. They provide timely and adequate information on the status of risk and controls to the Board and its Committees. All College risks are reviewed and approved by the Audit Committee in its quarterly meetings. The Audit Committee recommends the risks to the Board for review in its regular meetings.

The College uses a Risk Assessment Matrix that is compiled by Management for each key risk. Risk Register are clustered based on the remit of the College Committees. The clusters are: Board of Management, Learning & Teaching, and Business Resources and Infrastructure. There is no 'Risk Cluster' specifically identified for the Audit Committee since its accountabilities for management of all risks are indicated in the Committee's Terms of Reference.

The Risk Registers categorise risks as: Reputation risks, Political risks, Financial risks, Compliance / Regulatory risks, Learning and Teaching risks, and Other College services risks. Individual risks are assigned both a Lead committee and Lead officer.

Risks are assessed on a Likert type scale using 1 (low) to 5 (high). Risks (taking into account the mitigating controls) are scored for likelihood of occurrence and for degree of impact if it does occur. The risk score is the multiple of likelihood and impact. Risks are plotted on a heat map. The Board's appetite for the risk is illustrated via colour coding on the heat map. Risks are however not first scored without taking into account the mitigating controls (the inherent risk).

The Risk register indicates each risks description, owner, manager, risk description, areas of risk (which are bullet points that identify triggers and consequences), risk categories, risk appetite category and key elements, the previous and current risk assessment, two heat maps that include the appetite shaded with the relevant colour, the 'movement' required or treatment required for the risk (Mitigating actions to be taken, Current position acceptable, Current position can be relaxed), 'movement in period' or the status changes of the risk (new risk, increased risk score, no change, decreased risk score, the risk is now closed), existing controls are listed as a narrative.

Refresher training on the College's risk management policy and methodology takes place on a regular basis. The College's risk management methodology was recently communicated to the College Operations Group (via a presentation) on 22 February 2018 and to new Board of Management members on 25 October 2018. There have been a number of communications to ensure key staff understand their responsibilities for managing risks.

SCOPE AND APPROACH:

The scope of this review was to assess whether:

- A suitable risk strategy and policy is in place;
- The structure, roles, and responsibilities for risk management are clear, including the respective roles and responsibilities of the Board, Audit Committee and Management;
- Ayrshire College has robust systems for identifying and evaluating all significant strategic and operational risks;
- Mitigating controls, net risk and target risk are sufficiently identified and agreed;
- The reporting arrangements in place for risk management are appropriate;
- Appropriate risk management training is being provided.

Our approach included the review of key documentation in relation to risk management and enquiries with key staff to assess whether appropriate controls are in place, and whether existing controls are operating effectively. We also assessed Ayrshire College's Risk Management Policy and Methodology against our risk management maturity assessment model. Our summary assessment of the Commission's risk management maturity is shown in an Excel document provided separately.

GOOD PRACTICE:

Ayrshire College has embraced risk management methodologies and has a clear Policy and Methodology. They making effective use of heat maps, risk scoring, and risk treatment in the risk registers. The heat maps with risk appetite colour coding help illustrate the degree to which a risk falls outside of the appetite. The registers also provide clear guidance on the risk treatment. Each risk includes descriptors identifying triggers, consequences, as well as controls and actions. All risks have owners and managers and the registers are formally reviewed quarterly.

New board members are trained on the College's risk management arrangements. The training includes the Board's accountabilities for overseeing risk management.

KEY FINDINGS:

Whilst we identified good practice within the risk management program, our review identified one area where further improvements could be made to the current risk management processes and documentation.

CONCLUSION:

At this stage, we can provide substantial assurance over the design and substantial assurance over the operational effectiveness of the risk management controls in place at Ayrshire College. This is the highest level of assurance we provide. We recommend that Management implements the noted control improvement to further develop the risk management arrangements, and enable identification of the degree to which controls are relied upon to mitigate key risks.

In conclusion, we have assessed the Ayrshire's risk management maturity as Enabled on the whole. With only one of the five aspects assessed as Managed the second highest level. This scoring reflects the opportunity for improvement identified above to achieve high quality risk management practices. The definitions used in our risk management maturity assessment model are shown in Appendices II and IV. The full model can be used by management to plan, monitor and report on risk management improvements. Internal Audit will periodically review risk management maturity and assess the continuing operation of the risk management arrangements.

OUR TESTING DID NOT IDENTIFY ANY CONCERNS SURROUNDING THE CONTROLS IN PLACE TO MITIGATE THE FOLLOWING RISKS:

- ✓ Ayrshire College may not have set out clearly its strategic direction and objectives in relation to risk management (including policy, roles and responsibilities, objectives and communication);
- ✓ Ayrshire College may not have adopted a systematic process in identifying, evaluating and measuring its key strategic and operational risks;
- ✓ Ayrshire College may not have adequate reporting to its committees and the Management in relation to risk management activities.
- ✓ Ayrshire College may not be providing appropriate risk management training.

DETAILED FINDINGS

RISK: AYRSHIRE COLLEGE MAY NOT HAVE ADOPTED A SYSTEMATIC PROCESS IN IDENTIFYING, EVALUATING AND MEASURING ITS KEY STRATEGIC AND OPERATIONAL RISKS;

Ref	Sig.	Finding
1		When evaluating risk impact and likelihood, it is good practice to assess the risk first without considering mitigating controls (i.e., inherent risk). Then, the risk should be assessed taking into consideration the mitigating controls (i.e., residual risk). The delta between the inherent and residual risks indicate the assessed effectiveness of the mitigating controls and the degree to which the organisation is relying on the controls. The risk management methodology at the College does not require calculating or reporting of an inherent risk score. There is a risk that if the inherent risk score is not calculated or reported, that it's difficult to ascertain the extent to which the controls are effective and efficient and the degree to which they are relied upon. For example, if the inherent risk score is 15 (5 likelihood x 3 impact), and that falls within the risk appetite, but the residual risk (taking into account one control) score is 14, then the control may not require. Or, if the inherent risk score is 25 (5 likelihood x 5 impact) and the residual risk is 15, and there is only one control, then it's clear that the control is believed to be significantly mitigating the risk. That control could be a priority for internal audit assurance testing.

RECOMMENDATION:

Include inherent risk scores in the methodology and registers.

MANAGEMENT RESPONSE:

We will include the inherent risk score within the detailed risk matrix of each risk.

Responsible Officer:	***Director of Finance and Student Funding***
Implementation Date:	***31 March 2019***

OBSERVATIONS

RISK MANAGEMENT TOOL

There are a number of tools that automate risk management activities. Most tools maintain the inherent and residual risk scores, plot the risks on heat maps, track risk owners and managers, map mitigating controls with their risks, record control owners, track effective evaluation of controls and record action plans, and produce interactive dashboards.

The College's risk management process is manually generated. The inherent score isn't calculated or included on the reports and the controls aren't mapped to a specific risk trigger or consequence.

Implementing a risk management tool could reduce the time required to complete risk management activities and reporting. It enables the College to implement inherent risk calculation and reporting and to implement additional features (such as tracking action plans and producing interactive dashboards). The tool may help ensure that the risk management process is consistently applied across multiple areas, though we identified no evidence of the process being applied inconsistently within the College.

This observation is included as a possible process improvement. We have not raised it as a finding because we do not consider it to be a significant risk to the successful operation of the risk management processes.

APPENDIX I STAFF INTERVIEWED

BDO LLP APPRECIATES THE TIME PROVIDED BY ALL THE INDIVIDUALS INVOLVED IN THIS REVIEW AND WOULD LIKE TO THANK THEM FOR THEIR ASSISTANCE AND COOPERATION.

James Thomson	Director of Finance and Student Funding

APPENDIX II – DEFINITIONS

LEVEL OF ASSURANCE	DESIGN OF INTERNAL CONTROL FRAMEWORK		OPERATIONAL EFFECTIVENESS OF CONTROLS	
	FINDINGS FROM REVIEW	DESIGN OPINION	FINDINGS FROM REVIEW	EFFECTIVENESS OPINION
Substantial	Appropriate procedures and controls in place to mitigate the key risks.	There is a sound system of internal control designed to achieve system objectives.	No, or only minor, exceptions found in testing of the procedures and controls.	The controls that are in place are being consistently applied.
Moderate	In the main there are appropriate procedures and controls in place to mitigate the key risks reviewed albeit with some that are not fully effective.	Generally a sound system of internal control designed to achieve system objectives with some exceptions.	A small number of exceptions found in testing of the procedures and controls.	Evidence of non-compliance with some controls that may put some of the system objectives at risk.
Limited	A number of significant gaps identified in the procedures and controls in key areas. Where practical, efforts should be made to address in-year.	System of internal controls is weakened with system objectives at risk of not being achieved.	A number of reoccurring exceptions found in testing of the procedures and controls. Where practical, efforts should be made to address in-year.	Non-compliance with key procedures and controls places the system objectives at risk.
No	For all risk areas there are significant gaps in the procedures and controls. Failure to address in-year affects the quality of the organisation's overall internal control framework.	Poor system of internal control.	Due to absence of effective controls and procedures, no reliance can be placed on their operation. Failure to address in-year affects the quality of the organisation's overall internal control framework.	Non compliance and/or compliance with inadequate controls.

RECOMMENDATION SIGNIFICANCE	
High	A weakness where there is substantial risk of loss, fraud, impropriety, poor value for money, or failure to achieve organisational objectives. Such risk could lead to an adverse impact on the business. Remedial action must be taken urgently.
Medium	A weakness in control which, although not fundamental, relates to shortcomings which expose individual business systems to a less immediate level of threatening risk or poor value for money. Such a risk could impact on operational objectives and should be of concern to senior management and requires prompt specific action.
Low	Areas that individually have no significant impact, but where management would benefit from improved controls and/or have the opportunity to achieve greater effectiveness and/or efficiency.

APPENDIX III - TERMS OF REFERENCE

PURPOSE OF REVIEW:

As part of the 2018 - 2019 Internal Audit Plan, it was agreed that internal audit would review the risk management framework in place within Ayrshire College and compare this with good practice.

The purpose of this review is to provide the Audit Committee with a level of assurance around the current arrangements, and provide management with advice and recommendations for improving the arrangements further. The deliverables will include an internal audit report and also a populated risk management maturity model, to demonstrate to management in detail the maturity status and actions which can be taken to further develop the risk management processes.

KEY RISKS:

Based upon the risk assessment undertaken during the development of the internal audit operational plan, through discussions with management, and our collective audit knowledge and understanding the key risks associated with the area under review are:

- Ayrshire College may not have set out clearly its strategic direction and objectives in relation to risk management (including policy, roles and responsibilities, objectives and communication);
- Ayrshire College may not have adopted a systematic process in identifying, evaluating and measuring its key strategic and operational risks;
- Ayrshire College may not have adequate reporting to its committees and the Management in relation to risk management activities.
- Ayrshire College may not be providing appropriate risk management training.

SCOPE OF REVIEW:

The following areas will be covered as part of this review:

- To assess whether a suitable risk strategy and policy is in place;
- To assess whether the structure, roles, and responsibilities for risk management are clear, including the respective roles and responsibilities of the Board, Audit & Risk Committee and Management;
- To assess whether Ayrshire College has robust systems for identifying and evaluating all significant strategic and operational risks;
- To assess whether mitigating controls, net risk and target risk are sufficiently identified and agreed;
- To assess whether the reporting arrangements in place for risk management are appropriate;
- To assess whether appropriate risk management training is being provided.

However, Internal Audit will bring to the attention of management any points relating to other areas that come to their attention during the course of the audit. We assume for the purposes of estimating the number of days of audit work that there is one control environment, and that we will be providing assurance over controls in this environment. If this is not the case, our estimate of audit days may not be accurate.

FOR MORE INFORMATION:

RUTH IRELAND

+44 (0)20 7893 2337
ruth.ireland@bdo.co.uk

www.bdo.co.uk

AYRSHIRE COLLEGE

INTERNAL AUDIT REPORT

IT SECURITY
JANUARY 2019

LEVEL OF ASSURANCE	
Design	Operational Effectiveness
Moderate	Moderate

BDO

AYRSHIRE COLLEGE, IT SECURITY

DISTRIBUTION	
Brad Johnstone	Head of ICT
James Thomson	Director of Finance and Student Funding
Audit Committee	Members

REPORT STATUS LIST	
Auditors:	Sean Morrison
Dates work performed:	27 November - 11 December 2018
Draft report issued:	21 December 2018
Final report issued:	23 January 2019

AYRSHIRE COLLEGE, IT SECURITY

EXECUTIVE SUMMARY

LEVEL OF ASSURANCE: (SEE APPENDIX I FOR DEFINITIONS)

Design	■	Generally a sound system of internal control designed to achieve system objectives with some exceptions.
Effectiveness	■	Evidence of non-compliance with some controls, that may put some of the system objectives at risk.

SUMMARY OF RECOMMENDATIONS: (SEE APPENDIX I)

High	▲	0
Medium	■	1
Low	●	5

TOTAL NUMBER OF RECOMMENDATIONS: 6

BACKGROUND:

As part of the 2018 – 2019 Internal Audit plan, it was agreed that internal audit would carry out a high-level assessment of network IT security controls to ensure that the confidentiality, integrity and availability of Ayrshire College's systems and data are maintained.

The Ayrshire College IT Team is overseen by the Head of ICT, who manages a team of two ICT Team Leaders, ten ICT Technicians, the IT Help Desk Administrator and an ICT Officer. Together the team is responsible for the maintenance and development of the Ayrshire College IT network, security, and ensuring that the College's IT services are functioning as required for the staff and students.

The Scottish Government required all public bodies to have achieved Cyber Essentials accreditation by the end of October 2018. Ayrshire College has undertaken the required level of accreditation, through the completion of the Cyber Essentials questionnaire, and now plans to undertake the process for achieving the Cyber Essentials Plus accreditation. This will consist of Barrier Networks carrying out an audit on the IT infrastructure in early December 2018. If awarded, re-assessments will occur on an annual basis for maintaining the plus accreditation.

Ayrshire College has a number of IT policies and procedures in place including IT Security, Staff Acceptable Use and Network Security. Within the documents the roles and responsibilities are detailed, including those of the Head of ICT, the IT Team Leaders and other general users. The documents have recently been updated and are made available to staff via the College's staff intranet, within the policies and procedures section.

AYRSHIRE COLLEGE, IT SECURITY

Administrator access to the internal network is centrally controlled. Ayrshire College has individual access logins for all admin access rights, held by select ICT staff, and the default administrator account is locked down. Requests for access for new starts, alterations to access rights and removal of leavers' rights come from the HR department, who raise a ticket on the bespoke HR portal. The tickets can only be actioned by the ICT team, who would do so only if the request had appropriate line manager approval and additional required information, such as access rights to be applied and staff information. Following the date of any required action the IT Service Desk Administrator conducts checks to verify that the actions have been completed by the ICT department.

Network password settings are configured within the active directory for all users. The settings state that users have a maximum password age of 90 days, with a minimum of eight characters. The last ten passwords are remembered and passwords are required to be complex.

Third party network access follows a similar process to new employees, in that an account is set up within the active directory and disabled when work is not required, or removed if the external party is no longer used. Access expires based upon the period of time that was originally requested and authorised to complete the required task. Guest wireless access is available for users and this has been completely segregated from the corporate network. Eduroam is also in place, and is utilised by staff and students with WPA2 encryption and password requirements in place. This provides unique encryption keys for each wireless client that connects to the network. The wireless access also utilises SSID broadcasting to make the connections searchable by user devices.

Patching is conducted by the senior ICT staff on the Windows Estate, using WSUS, SolarWinds for the servers and Sysaid for the clients. The Mac's are patched using the patch management software Jamf. Patching is conducted following the completion of the College's backup, to ensure that if there are any issues roll back will be effective, as the College do not have a test environment for patching.

The ICT Team also conducts regular internal vulnerability scanning through the use of the software Nessus. By running these scans the IT team is able to generate reports highlighting vulnerabilities within the network, for example if devices or computers do not have the most up to date updates installed on them. The ICT staff then use the reports to conduct any mitigating actions on the vulnerabilities identified.

The College's perimeter firewall (Fortinet), controls the flow of network traffic and provides a first line of defence against external attacks on the network. Fortinet has best practice functionality, such as having Forti analyser, which takes logs from every device on the network and allows the ICT staff to monitor traffic on the network to identify threats, which is done on a daily basis.

There are physical and environmental security controls operating at the three server rooms (two in Kilmarnock campus, and one in Ayr campus) such as, fob only access to the Kilmarnock campus and code locks at the Ayr campus, all of which can only be accessed by the ICT staff and the Estates staff in the case of an emergency. The server rooms also have air conditioning, CCTV in the halls, fire protection, clear dedicated rooms and software "SolarWinds" which monitors the server status and temperature.

Security software "Eset" has been deployed as the end-point security solution for the network. This includes anti-virus for all devices on the network and scanning on all removable devices, and is centrally configured, being updated on a daily basis at least three times a day, and is managed and monitored by the ICT Team. The email scanning solution

AYRSHIRE COLLEGE, IT SECURITY

used by Ayrshire College is Office 365, which can detect and remove viruses and spam when required, and this is also monitored by the ICT Team.

"Veeam" is the primary backup software for the server/system backup, and the College has a Microsoft Hyper V-virtual infrastructure. Veeam is installed on a physical server located at each site. If the primary server fails, the ability to restore is available from one of the other servers. The backups have been configured to a target HPE StoreOnce System which dedupes and compresses the data. This data is then replicated to a partner HPE StoreOnce located at another site which creates two geographically dispersed copies of the backup data. The backups undertaken by the Head of ICT and the ICT Team Leaders, are conducted on a daily basis.

Disaster recovery tests are conducted throughout the year by the Head of ICT and the ICT Team Leaders, on areas such as the servers, the firewall, and storage capabilities.

SCOPE AND APPROACH:

Scope and Approach

The scope of this review was to assess whether:

- Network security policy and acceptable usage guidance has been developed and published.
- Powerful access to the network is controlled.
- There is effective user access and authorisation controls in place for staff and third parties, including the management of new starts, movers and leavers.
- Network password settings are in line with policy requirements and best practice recommendations.
- Remote access to the network is securely configured.
- Wireless access to the network is securely configured.
- There is regular security vulnerability scanning and network perimeter testing.
- Network devices are patched in line with supplier recommendations.
- Firewalls and other security appliances have been deployed and their configuration is securely administered and maintained.
- There are physical and environmental security controls in place for data hosting facilities.
- There is network security monitoring and filtering including: anti-virus, mail scanning and internet content filtering.
- Network data is backed-up and securely stored in line with business requirements.
- Effective IT disaster recovery arrangements have been implemented.
- Effective network security monitoring, logging and incident response procedures have been implemented.

Our approach was to conduct interviews to establish the controls in operation for each of our areas of audit work. We then sought documentary and system-based evidence that these controls were operating as designed as described. We evaluated these controls to identify whether they adequately address the risks, and utilising our tools and techniques, we tested the controls for operating effectiveness.

AYRSHIRE COLLEGE, IT SECURITY

GOOD PRACTICE:

A number of areas of good practice were noted during the review including, but not limited to:

- The corporate, student and guest wireless networks are logically separated and encrypted.
- There are strong firewalls in place that are active pairs, and also provide failover capabilities for the other. The firewall in place also has a log in place for staff to monitor network activity.
- End-point software with anti-virus capability has been deployed to protect the network from malicious software.
- Mail scanning solutions have been deployed to protect the network.
- Third parties are prevented from direct remote access to the network with all instances of access being supervised by IT.
- There is regular internal security vulnerability scanning undertaken on the network and devices through the use of Nessus.
- There are strong physical and environmental controls in place for the server rooms.
- The IT infrastructure in place has strong backup and disaster recovery capabilities.

KEY FINDINGS:

Notwithstanding the elements of good practice noted above we have found six areas where further improvements could be made. We have listed these improvements below. We would ask the Committee to note that the number of findings raised shows strong performance in IT security in comparison to similar organisations reviewed:

1) **Policies and procedures -** We identified the following areas where improvements could be made to strengthen the IT policies and procedures in place:
    a) Guidance procedures for all key functions conducted by the ICT team, such as patching, network scanning/vulnerability scanning with timescales for priorities and backups are not demonstrated.
    b) At the time of the audit a number of the policies have not been updated to take account of GDPR. In particular the Data Protection Policy was still outdated, despite the May 2018 implementation date for GDPR.
    c) There is no requirement for staff to verify that they have read and acknowledged the IT policies and procedures in place.
    d) A monthly security review is undertaken, and demonstrates good practice. However, the tasks within the review have not been documented to guide staff on what is required to be completed.
2) **Account lockout policy -** Currently there is no account lockout set within the password settings utilised at the College. We recognise that the College has taken this approach to ensure that no students get locked out of their accounts and there is software (Netrix) which will be implemented to allow monitoring of login attempts.
3) **Tracking of requests -** During our sample testing of new starts and leavers access to the college network, it was evident that the current process for retrospectively accessing tickets requesting and authorising alterations to the users on the active directories is very time consuming and inefficient. This is particularly due to the bespoke HR system for raising requests only holding the last twenty requests, and the current service desk system (spiceworks) not being used for new starts and leavers requests.

AYRSHIRE COLLEGE, IT SECURITY

4) **Mobile device management -** Ayrshire College does not currently have a mobile device management solution in place. We recognise that staff do not all have access to mobile devices and that use on the devices is mainly limited to email access. Also, we note that the IT team is aware that this is an area that can be improved. The College is exploring options for procuring a mobile device management package in early 2019.
5) **USB's -** Our audit found that staff and students are able to make use of USB devices on the network. We recognise that Eset scans all removable devices for viruses when inserted into a machine on the network, mitigating the risk of viruses being introduced to the college network.
6) **Patches -** Our audit noted that there is currently no documented testing in a dedicated test environment for patches before these are deployed to the live environment. There is also no formalised process for patching documented.

CONCLUSION:

At this stage, we can provide moderate assurance over the design and operational effectiveness of the controls in place in relation to IT security. We recommend that management implements the noted control improvements within this report, and ensure that the controls in place operate consistently across the organisation.

AYRSHIRE COLLEGE, IT SECURITY

DETAILED FINDINGS

RISK: A CONSISTENT AND POLICY DRIVEN APPROACH HAS NOT BEEN IMPLEMENTED TO MAINTAIN NETWORK SECURITY.

Ref	Sig.	Finding
1		**Policies and Procedures** It is important that Ayrshire College's policies and procedures provide clear guidance of the IT processes adopted by the organisation, sufficient to promote consistent and effective practices and provide clear direction to management and staff on the management of IT related risks. We identified the following areas where improvements could be made to strengthen the IT policies and procedures in place: • There are no documented guidance procedures in place for all key functions conducted by the ICT departments, such as patching, network scanning/vulnerability scanning with timescales for priorities backups etc. • Not all policies have been formally updated to take account of GDPR. In particular the Data Protection Policy was still to be approved. • There is no requirement for staff to verify that they have read and acknowledged the IT policies and procedures in place. • A monthly security review is undertaken, and demonstrates good practice. However, the tasks within the review have not been documented to guide staff on what is required to be completed. We found that the IT Team is very experienced, and capable of carrying out its roles and responsibilities. However, there is a risk that the current policies and procedures are limited in their ability to provide staff with clear direction to support the management of the IT infrastructure in place, in particular new staff who are not accustomed to the processes at Ayrshire College.

RECOMMENDATION:

We recommend that Ayrshire College takes the following steps to improve the effectiveness of the IT policies and procedures in place:

- Guidance procedures should be created for all key activities undertaken by the IT department, such as patching, network scanning, and backups.
- All policies to be updated to reflect any relevant and current legislations, such as GDPR.
- A process to be put in place for new staff to verify that they have read and will abide by all IT policies and procedures.
- The monthly security review should be documented, to ensure that all IT staff know what checks are required, to mitigate the risk of personal knowledge being lost.

AYRSHIRE COLLEGE, IT SECURITY

MANAGEMENT RESPONSE:	
Agreed. Guidance procedures and monthly security reviews will be documented by 15 March 2019. Policies will be updated engaging with stakeholders where required.	
Responsible Officer:	Head of ICT
Implementation Date:	31 August 2019

AYRSHIRE COLLEGE, IT SECURITY

RISK: THERE IS A LACK OF CONTROL OVER HOW STAFF, THIRD PARTIES AND OTHER STAKEHOLDERS GAIN ACCESS TO THE COLLEGE'S NETWORK.		
Ref	Sig.	Finding
2		**Account Lockout Policy** Our audit found that current account lockout settings can be improved to strengthen network logical access controls and to ensure that these are in line with best practice. Currently there is no account lockout set within the password settings utilised at the College. We recognise that the College has taken this approach to ensure that no students are locked out of their accounts. There is software (Netrix) which will be implemented to allow monitoring of login attempts. However, there is a risk that by not following best practice that weak account lockout settings could result in unauthorised users gaining access to the network.

RECOMMENDATION:

We recommend that the College follows best practice for account access and add lockout settings to the password policy. Appendix IV has an example of good practice within the sector.

MANAGEMENT RESPONSE:

Not accepted.

Locking users out is detrimental to some of our most vulnerable and ASN students. The College has therefore deliberately chosen to not impose lockout settings. The software required the College to have the same settings for all users.

The Internal Auditors have recognised the additional robust password and account settings in place within the College.

Responsible Officer:	N/A
Implementation Date:	N/A

AYRSHIRE COLLEGE, IT SECURITY

RISK: THERE IS A LACK OF CONTROL OVER HOW STAFF, THIRD PARTIES AND OTHER STAKEHOLDERS GAIN ACCESS TO THE COLLEGE'S NETWORK.		
Ref	Sig.	Finding
3		**Access Requests Audit Trail** Being able to retrospectively access the backup evidence for making alterations and additions to users on the active directory is essential for ensuring that all changes have been made with proper authorisation. During our sample testing of new starts and leavers access to the College network, it was evident that the current process for retrospectively accessing tickets requesting and authorising alterations to the users on the active directories is very time consuming and inefficient. This is particularly due to the bespoke HR system for raising requests only holding the last twenty requests, and the current service desk system (spiceworks) not being used for new starts and leavers requests. We recognise that the College plans to implement the Sysaid service desk system in the near future, which has the capability to show workflows and allow documents to be attached, improving the audit trail. However, there is a risk that retrospective verification of alterations to the users on the active directory cannot be done due to the inefficient process for storing backup evidence.

RECOMMENDATION:
We recommend that a process is put in place to ensure easy access to all backup evidence required to verify the request and authorisation for alterations or additions of users on the active directory.

MANAGEMENT RESPONSE:	
Agreed. The College will address this as part of the implementation of the Sysaid service desk system.	
Responsible Officer:	Head of ICT
Implementation Date:	31 August 2019

AYRSHIRE COLLEGE, IT SECURITY

RISK: NETWORK DEVICES ARE NOT EFFECTIVELY DEPLOYED, MONITORED OR MANAGED.		
Ref	Sig.	Finding
4		**Mobile Device Management** Mobile device management provides IT managers with central control of devices in a corporate network, including device data, security, the capability of killing the device, and data transmission monitoring. Ayrshire College does not currently have a mobile device management solution in place. We recognise that staff do not all have access to mobile devices and that use on the devices is mainly limited to email access. Also, we note that the IT team is aware that this is an area that can be improved and the College is exploring options for procuring a solution. Nonetheless, there is a risk that mobile devices within the network are currently vulnerable to external threats.

RECOMMENDATION:

We recommend that the College procures a mobile device management package and apply it to all college mobile devices on the network.

MANAGEMENT RESPONSE:

The College will review the options available and the added value of a mobile device management package.

Responsible Officer:	Head of ICT
Implementation Date:	30 June 2019

AYRSHIRE COLLEGE, IT SECURITY

RISK: NETWORK DEVICES ARE NOT EFFECTIVELY DEPLOYED, MONITORED OR MANAGED.		
Ref	Sig.	Finding
5		**USB Devices** USB's provide the ability to store files in a portable manner for use on different devices, which is essential in the education sector. However, USBs pose the risk of introducing viruses into a network, and the loss of sensitive data if not effectively controlled. Our audit found that staff and students are able to use USB devices on the network. We recognise that Eset scans all removable devices for viruses when inserted into a machine on the network, mitigating the risk of viruses being introduced to the college network. We also recognise that due to the nature of the education sector staff and students use removable storage devices to carry out their roles, and that the College cannot specifically ban the use of USBs, until the adoption of the home drives and cloud storage are utilised by all network users. Nonetheless, there is a risk that if staff USBs are lost or stolen that any sensitive information contained within the device could be lost or utilised illegally, particularly if the device is not sufficiently encrypted.

RECOMMENDATION:

We recommend that the following best practice areas are adopted if the College decides to continue to allow the use of removable storage devices:

- Enforce the USB procedures detailed within the current IT Security Policy, and provide training that describes the controls and uses of USBs.
- Ensure that all USBs used by staff are encrypted, password protected, and deploy remote wiping technology on the USBs

MANAGEMENT RESPONSE:

These recommendations will be addressed as part of the work to review and update existing policies.

Training in the use of USBs and ICT security will be addressed within the College's ongoing GDPR and data protection work.

Responsible Officer:	Head of ICT
Implementation Date:	31 August 2019

AYRSHIRE COLLEGE, IT SECURITY

RISK: NETWORK DEVICES ARE NOT EFFECTIVELY DEPLOYED, MONITORED OR MANAGED.		
Ref	Sig.	Finding
6		**Patch Management** Our audit noted that there is currently no testing in a dedicated test environment for patches before these are deployed to the live environment. There is also no formalised process for patching documented. We recognise that the current process consists of a controlled process of patching servers following the completion of the daily backup, which ensures that if any issues occur then the IT team can roll back everything prior to the updated being applied. Nonetheless there is a risk that patches deployed to the network may result in unexpected downtime for network users.

RECOMMENDATION:

We recommend that a feasibility study is undertaken on adopting a test environment for the patch management within the College.

We also recommend that the patching process is documented.

MANAGEMENT RESPONSE:

Agreed.
Existing patching processes will be documented by 15 March 2019.

A feasibility study will be undertaken.

Responsible Officer:	Head of ICT
Implementation Date:	15 March 2019

AYRSHIRE COLLEGE, IT SECURITY

OBSERVATIONS

EXTERNAL NETWORK PENETRATION TESTING

The college do not currently conduct external network penetration testing. We note however that the internal controls in place such as internal vulnerability scanning, robust firewalls and anti-virus software, support a strong internal defence against any threats. Also, as part of the annual Cyber Essentials Plus accreditation audit, to be conducted by Barrier Networks in early December 2018, the testing will include an external network penetration test.

AYRSHIRE COLLEGE, IT SECURITY

APPENDIX I - STAFF INTERVIEWED

BDO LLP APPRECIATES THE TIME PROVIDED BY ALL THE INDIVIDUALS INVOLVED IN THIS REVIEW AND WOULD LIKE TO THANK THEM FOR THEIR ASSISTANCE AND COOPERATION.

Brad Johnstone	Head of ICT
David Keenan	ICT Team Leader
Gillian McClue	ICT Helpdesk Administrator
James Barnes	ICT Team Leader

AYRSHIRE COLLEGE, IT SECURITY

APPENDIX II – DEFINITIONS

LEVEL OF ASSURANCE	DESIGN OF INTERNAL CONTROL FRAMEWORK		OPERATIONAL EFFECTIVENESS OF CONTROLS	
	FINDINGS FROM REVIEW	DESIGN OPINION	FINDINGS FROM REVIEW	EFFECTIVENESS OPINION
Substantial 	Appropriate procedures and controls in place to mitigate the key risks.	There is a sound system of internal control designed to achieve system objectives.	No, or only minor, exceptions found in testing of the procedures and controls.	The controls that are in place are being consistently applied.
Moderate 	In the main there are appropriate procedures and controls in place to mitigate the key risks reviewed albeit with some that are not fully effective.	Generally a sound system of internal control designed to achieve system objectives with some exceptions.	A small number of exceptions found in testing of the procedures and controls.	Evidence of non compliance with some controls, that may put some of the system objectives at risk.
Limited 	A number of significant gaps identified in the procedures and controls in key areas. Where practical, efforts should be made to address in-year.	System of internal controls is weakened with system objectives at risk of not being achieved.	A number of reoccurring exceptions found in testing of the procedures and controls. Where practical, efforts should be made to address in-year.	Non-compliance with key procedures and controls places the system objectives at risk.
No 	For all risk areas there are significant gaps in the procedures and controls. Failure to address in-year affects the quality of the organisation's overall internal control framework.	Poor system of internal control.	Due to absence of effective controls and procedures, no reliance can be placed on their operation. Failure to address in-year affects the quality of the organisation's overall internal control framework.	Non compliance and/or compliance with inadequate controls.

RECOMMENDATION SIGNIFICANCE	
High 	A weakness where there is substantial risk of loss, fraud, impropriety, poor value for money, or failure to achieve organisational objectives. Such risk could lead to an adverse impact on the business. Remedial action must be taken urgently.
Medium 	A weakness in control which, although not fundamental, relates to shortcomings which expose individual business systems to a less immediate level of threatening risk or poor value for money. Such a risk could impact on operational objectives and should be of concern to senior management and requires prompt specific action.
Low 	Areas that individually have no significant impact, but where management would benefit from improved controls and/or have the opportunity to achieve greater effectiveness and/or efficiency.

AYRSHIRE COLLEGE, IT SECURITY

APPENDIX III - TERMS OF REFERENCE

PURPOSE OF REVIEW:

The purpose of this review is to carry out a high-level assessment of network IT security controls to ensure that the confidentiality, integrity and availability of Ayrshire College's systems and data are maintained.

KEY RISKS:

Based upon the risk assessment undertaken, discussions with management, and our collective audit knowledge and understanding the key risks under review within this area are:

- A consistent and policy driven approach has not been implemented to maintain network security;
- There is a lack of control over how staff, third parties and other stakeholders gain access to the College's network;
- Network infrastructure devices are not securely configured;
- Network devices are not effectively deployed, monitored or managed;
- The network is not adequately protected from external threats;
- Resilience and redundancy considerations are not built into the network; and
- Security incident monitoring and response procedures are ineffective.

SCOPE OF REVIEW:

The scope of this review will be to assess whether:

- Network security policy and acceptable usage guidance has been developed and published;
- Powerful access to the network is controlled;
- There is effective user access and authorisation controls in place for staff and third parties, including the management of new starts, movers and leavers;
- Network password settings are in line with policy requirements and best practice recommendations;
- Remote access to the network is securely configured;
- Wireless access to the network is securely configured;
- Network devices are built and deployed in a secure manner;
- Security vulnerability scanning and network perimeter testing is conducted on a planned basis;
- Network devices are patched in line with supplier recommendations;
- Firewalls and other security appliances have been deployed and their configuration is securely administered and maintained;
- There are physical and environmental security controls in place for data hosting facilities;
- There is network security monitoring and filtering including: anti-virus, mail scanning and internet content filtering;
- Network data is backed-up and securely stored in line with business requirements;
- Effective IT disaster recovery arrangements have been implemented; and
- Effective network security monitoring, logging and incident response procedures have been implemented.

AYRSHIRE COLLEGE, IT SECURITY

APPENDIX IV - PASSWORD POLICY BEST PRACTICE

Policy	Leading Practice
Minimum Password Length	8 or greater
Effective Minimum Password Length	8 or greater
Maximum Password Age in Days	30 to 60
Minimum Password Age in Days	0
Password History Size	22 or greater
Password Complexity	Enabled
Reversible Password Encryption	Disabled
Lockout Threshold	3
Lockout Duration	0
Reset Lockout Counter in Minutes	1440
Force Logoff When Logon Time Expires	Enabled
Rename Administrator Account	New Name
Rename Guest Account	New Name
Allow Lockout of Local Administrator Account	Enabled
Disable Password Changes for Machine Accounts	Disabled

FOR MORE INFORMATION:

RUTH IRELAND

+44 (0)20 7893 2337
ruth.ireland@bdo.co.uk

www.bdo.co.uk

AYRSHIRE COLLEGE

INTERNAL AUDIT REPORT – DRAFT

FINANCIAL PLANNING
FEBRUARY 2019

LEVEL OF ASSURANCE	
Design	Operational Effectiveness
Substantial	Substantial

AYRSHIRE COLLEGE, FINANCIAL PLANNING

DISTRIBUTION	
Michael Breen	Vice Principal-Finance and Skills
James Thomson	Director of Finance and Student Funding
Liz Walker	Head of Financial Services
Audit Committee	

REPORT STATUS LIST	
Auditors:	Chloe Ridley
Dates work performed:	28 January - 01 February 2019
Draft report issued:	08 February 2019
Final report issued:	13 February 2019

AYRSHIRE COLLEGE, FINANCIAL PLANNING

EXECUTIVE SUMMARY

LEVEL OF ASSURANCE: (SEE APPENDIX I FOR DEFINITIONS)

Design	●	There is a sound system of internal control designed to achieve system objectives.
Effectiveness	●	The controls that are in place are being consistently applied.

SUMMARY OF RECOMMENDATIONS: (SEE APPENDIX I)

High	▲	0
Medium	■	0
Low	●	0

TOTAL NUMBER OF RECOMMENDATIONS: 0

BACKGROUND:

As part of the 2018-19 Internal Audit Plan, it was agreed that Internal Audit would review the design and operating effectiveness of the controls in place at Ayrshire College, "the College", surrounding financial planning arrangements.

Ayrshire College's budgeted income for 2018/19 was £51.64m, £41.44m of this comprises of Grant-in-Aid, £3.4m is tuition fees and £3.86m is education, commercial and other income. The College's budgeted expenditure for 2018/19 is £49.34m, £33.77m of this is salaries, £6.61m other operating expenses, £3.5m property costs and £5.34m Non-Profit Distributing (NPD) Contract and Private Finance Initiative (PFI) payments. This provides an operating surplus of £2.3m, however once depreciation of £2.2m is taken into consideration there is an expected surplus of £104k.

The largest areas of uncertainty for the College over the next few years are: the likelihood of significant increases in pay costs associated with annual cost of living pay awards with a standstill in SFC funding, and Scottish Government expectations that all colleges, on an annual basis, will deliver 3% efficiency savings (this equates to savings of circa £1,060,000 per annum).

The main assumptions in the 2018-19 budget were: 124,958 credit activity target, including 871 ESF funded credits, the lecturing staff budget built using the approved Curriculum Development Plan (CDP) 2018-19 (the organisational structure was used for all other staff cost assumptions), additional SFC funding of £1.1m towards Kilwinning PFI arrangements and £1.7m SFC funding for high priority back log maintenance works identified through the

AYRSHIRE COLLEGE, FINANCIAL PLANNING

sector condition survey published in Dec 2017. The College's 2017-18 budget and performance was used as a baseline in developing the 2018-19 budget.

The College's Financial Regulations state the following required approval process for the budget; the Vice Principal-Finance and Skills is responsible for preparing the budget for the approval of the Executive Management Team (EMT) prior to the consideration, scrutiny and approval of the Business, Resources and Infrastructure Committee (BRIC). The BRIC requires to recommend the budget to the Board of Management.

The College has 15 Directorates, each of which has its own budget. Two Team Leaders and a Financial Accountant within Finance that provides budget setting and monitoring support to budget holders. There are 13 Finance staff.

Finance use a budget timetable to assist with the budget process. It is prepared by the Head of Financial Services and is issued to relevant Finance staff.

SFC provides an indicative funding allocation in February. In March, Finance will prepare the draft budget, using the approved CDP and organisational structure.

Finance issue staff lists and budget templates to budget holders to complete and return in order to outline potential spend and activity in the coming year. Finance staff will then hold meetings with budget holders to challenge and discuss the rational for budgeted figures. The budget is updated to incorporate feedback from budget holders. In the 2018-19 budget setting process templates were not issued, Finance went straight to holding meetings with budget holders, due to the unusual situation that large savings that were required compared to prior years. Finance felt the situation should be discussed and made clear to budget holders from the outset of the process.

The final allocation of SFC funding is confirmed in May.

The budget is issued to the Vice Principal – Finance and Skills with updates made. The budget is then presented to the EMT, BRIC and the Board, in line with the requirements of the Financial Regulations.

SFC requires a 5 year Financial Forecast Return (FFR) to be submitted on an annual basis, normally with an end of September deadline. SFC issues a template which is to be completed and returned and guidance is provided on some of the key assumptions which should be made. Finance uses information gained within the budget setting process to prepare the FFR. Whilst the SFC requires a 5 year FFR to be produced, SFC funding continues to be provided on an annual basis, with no indication of what funding is planned in future years.

Finance performs scenario analyses on the FFR to consider the impact of changes in key assumptions, this includes: a reduction in the College's core credit allocation, a reduction in commercial income, an increase in staff salaries, and an increase in inflation.

The Financial Sustainability Plan 2019-21 indicates three options for consideration that were based on the amount of additional funding SFC provides. These options and the Plan have been presented to the Board, but are not yet available for the public. The options consider varying levels of voluntary severance dependent upon the level of funding the SFC provide to support PFI payments.

AYRSHIRE COLLEGE, FINANCIAL PLANNING

The control of income and expenditure within an agreed budget is the responsibility of the Budget Holder supported by the Director of Finance and Student Funding and the Finance Team.

Budget monitoring occurs on a monthly basis. Budget holders are assisted with their financial responsibilities by management information provided by Finance. Finance provides each budget holder with two reports about their budget: a Preview Report which shows spend in each month and any committed purchases, and a Budget Monitoring report which compares the budget position to year to date actual results and the reporting month's actual results. These responsibilities are included within Finance's month end checklist.

Team Leaders meet with budget holders on a monthly basis to provide support, challenge variances and determine the forecast year-end position.

The Vice Principal- Finance and Skills is responsible for supplying budgetary reports on all aspects of the College's finances to the EMT & BRIC. BRIC meet on a quarterly basis.

Management accounts are presented at every BRIC meeting, which includes the forecast year-end position which is considered on a quarterly basis The management accounts compare the budget to the budget month position, period to date position and full year forecast. The budget is not adjusted throughout the year. Explanations for any variances are included in the reports.

SCOPE AND APPROACH:

The scope of our review is to assess whether:

- Financial plans are based on reasonable assumptions and forecasts and accurate, reliable information;
- Financial plans are developed in a timely manner with appropriate consultation, review and approval arrangements;
- Scenario planning and sensitivity analysis has been carried out to ensure budgets are flexible and robust enough to meet organisational requirements and respond to funding changes; and
- Budget reforecasts are carried out on a regular basis to reflect changes which may occur to plans, or to predict the outturn where expenditure in some areas differs from expectations.

Our approach was to conduct interviews to establish the controls in operation for each of our areas of audit work. We then sought documentary evidence that these controls are designed as described. We evaluated these controls to identify whether they adequately address the risks.

During the course of the review we kept management informed of any issues which arise as a result of our testing.

A de-brief meeting was undertaken before completing the review on-site to discuss findings and initial recommendations.

AYRSHIRE COLLEGE, FINANCIAL PLANNING

GOOD PRACTICE:

We identified a number of areas of good practice:

A budget planning timetable is in place which acts as a financial planning tool, and details inputs required and deadlines. The budget is presented to the EMT, BRIC and the Board of Management as part of the budget approval process.

Meetings are held on a monthly basis with Finance and budget holders to provide support and to understand any variances that have arisen. Management accounts are presented to the BRIC on a regular basis.

CONCLUSION:

We are able to provide substantial assurance over the budget setting & monitoring arrangements in place within Ayrshire College.

OUR TESTING DID NOT IDENTIFY ANY CONCERNS SURROUNDING THE CONTROLS IN PLACE TO MITIGATE THE FOLLOWING RISKS:

- ✓ Financial plans may not be based on accurate, reliable or relevant information
- ✓ The financial planning process may not be carried out in a timely manner in accordance with a clearly defined timetable
- ✓ Financial plans may be based upon unreasonable assumptions or forecasts
- ✓ No, or limited, scenario planning or sensitivity analysis has been undertaken
- ✓ Budget reforecasts may not be carried out on a regular basis to reflect changes which may occur to plans, or to predict the outturn where expenditure in some areas differs from expectations
- ✓ Financial plans may not be subject to effective consultation, review or approval

AYRSHIRE COLLEGE, FINANCIAL PLANNING

STAFF INTERVIEWED	
BDO LLP APPRECIATES THE TIME PROVIDED BY ALL THE INDIVIDUALS INVOLVED IN THIS REVIEW AND WOULD LIKE TO THANK THEM FOR THEIR ASSISTANCE AND COOPERATION.	
James Thomson	Director of Finance and Student Funding
Liz Walker	Head of Financial Services
Michelle Hart	Finance Officer

AYRSHIRE COLLEGE, FINANCIAL PLANNING

APPENDIX I – DEFINITIONS

LEVEL OF ASSURANCE	DESIGN OF INTERNAL CONTROL FRAMEWORK		OPERATIONAL EFFECTIVENESS OF CONTROLS	
	FINDINGS FROM REVIEW	DESIGN OPINION	FINDINGS FROM REVIEW	EFFECTIVENESS OPINION
Substantial 	Appropriate procedures and controls in place to mitigate the key risks.	There is a sound system of internal control designed to achieve system objectives.	No, or only minor, exceptions found in testing of the procedures and controls.	The controls that are in place are being consistently applied.
Moderate 	In the main there are appropriate procedures and controls in place to mitigate the key risks reviewed albeit with some that are not fully effective.	Generally a sound system of internal control designed to achieve system objectives with some exceptions.	A small number of exceptions found in testing of the procedures and controls.	Evidence of non compliance with some controls, that may put some of the system objectives at risk.
Limited 	A number of significant gaps identified in the procedures and controls in key areas. Where practical, efforts should be made to address in-year.	System of internal controls is weakened with system objectives at risk of not being achieved.	A number of reoccurring exceptions found in testing of the procedures and controls. Where practical, efforts should be made to address in-year.	Non-compliance with key procedures and controls places the system objectives at risk.
No 	For all risk areas there are significant gaps in the procedures and controls. Failure to address in-year affects the quality of the organisation's overall internal control framework.	Poor system of internal control.	Due to absence of effective controls and procedures, no reliance can be placed on their operation. Failure to address in-year affects the quality of the organisation's overall internal control framework.	Non compliance and/or compliance with inadequate controls.

RECOMMENDATION SIGNIFICANCE	
High 	A weakness where there is substantial risk of loss, fraud, impropriety, poor value for money, or failure to achieve organisational objectives. Such risk could lead to an adverse impact on the business. Remedial action must be taken urgently.
Medium 	A weakness in control which, although not fundamental, relates to shortcomings which expose individual business systems to a less immediate level of threatening risk or poor value for money. Such a risk could impact on operational objectives and should be of concern to senior management and requires prompt specific action.
Low 	Areas that individually have no significant impact, but where management would benefit from improved controls and/or have the opportunity to achieve greater effectiveness and/or efficiency.

AYRSHIRE COLLEGE, FINANCIAL PLANNING

APPENDIX II - TERMS OF REFERENCE

PURPOSE OF REVIEW:

The purpose of this review is to provide management and the Audit Committee with assurance that Ayrshire College has well designed, effective controls in place in relation to financial planning.

KEY RISKS:

Financial plans may not be based on accurate, reliable or relevant information

The financial planning process may not be carried out in a timely manner in accordance with a clearly defined timetable

Financial plans may be based upon unreasonable assumptions or forecasts

No, or limited, scenario planning or sensitivity analysis has been undertaken

Budget reforecasts may not be carried out on a regular basis to reflect changes which may occur to plans, or to predict the outturn where expenditure in some areas differs from expectations

Financial plans may not be subject to effective consultation, review or approval

SCOPE OF REVIEW:

The scope of our review is to assess whether:

- Financial plans are based on reasonable assumptions and forecasts and accurate, reliable information;
- Financial plans are developed in a timely manner with appropriate consultation, review and approval arrangements;
- Scenario planning and sensitivity analysis has been carried out to ensure budgets are flexible and robust enough to meet organisational requirements and respond to funding changes; and
- Budget reforecasts are carried out on a regular basis to reflect changes which may occur to plans, or to predict the outturn where expenditure in some areas differs from expectations.

AYRSHIRE COLLEGE, FINANCIAL PLANNING

APPROACH:

Our approach will be to conduct interviews to establish the controls in operation for each of our areas of audit work. We will then seek documentary evidence that these controls are designed as described. We will evaluate these controls to identify whether they adequately address the risks.

We will seek to gain evidence of the satisfactory operation of the controls to verify the effectiveness of the control through use of a range of tools and techniques.

During the course of the review we will keep management informed of any issues which arise as a result of our testing.

A de-brief meeting will be undertaken before completing the review on-site to discuss findings and initial recommendations.

FOR MORE INFORMATION:

RUTH IRELAND

+44 (0)20 7893 2337
ruth.ireland@bdo.co.uk

www.bdo.co.uk

Ayrshire College

INTERNAL AUDIT PROGRESS REPORT 2018-19

February 2019

BDO

CONTENTS

EXECUTIVE SUMMARY

Introduction

The purpose of this report is to ***advise*** the Audit and Risk Committee of the progress of the Internal Audit Plan for 2018-19. This paper together with progress and assignment updates will be discussed with Management and the Audit and Risk Committee throughout the year. These reports will form the basis of information to support our Annual Internal Audit Report for 2018-19.

Internal Audit Plan 2018-19

Since the last Audit Committee meeting, the following internal audit report has been finalised, and is presented under separate cover:

- Risk Management
- Financial Planning
- IT Security

We have started the Estates and Infrastructure review.

Conclusion

The Audit Committee is asked to ***note*** this report.

WORK COMPLETED

Reports Issued	Overall Report Conclusions - see appendix I				
	▲	■	●	Design	Operational Effectiveness
Risk Management	0	0	1	Substantial	Substantial
Financial Planning	0	0	0	Substantial	Substantial
IT Security	0	1	5	Moderate	Moderate

PERFORMANCE AGAINST OPERATIONAL PLAN

Visit	Date of visit	Proposed Audit	Planned Days	Actual Days	Status
1	October 2018	Risk Management	5	5	Completed
2	January 2019	Financial controls – financial planning and longer term forecasting	5	5	Completed
3	February 2019	Estates and infrastructure	5		In progress
4		SFC returns	5		Fieldwork scheduled for April 2019
5		Student experience / curriculum review	5		Fieldwork scheduled for May 2019
6	November 2018	IT security	7	7	Completed
7		Follow up	3		Fieldwork scheduled for June 2019
TOTAL			**35**	**17**	

AUDIT PERFORMANCE

AUDIT	COMPLETION OF FIELDWORK	DRAFT REPORT	FINAL MANAGEMENT RESPONSES	FINAL REPORT
Risk Management	26 October 2018	12 November 2018	27 November 2018	30 November 2018
Financial Planning	1 February 2019	8 February 2019	13 February 2019	13 February 2019
IT Security	11 December 2018	21 December 2018	22 January 2019	23 January 2019

On average:

- Report issued in draft within 10 working days of completion of our fieldwork and a debrief meeting with management.
- Initial responses anticipated within 10 working days of the draft report being issued.

APPENDIX I - DEFINITIONS

LEVEL OF ASSURANCE	DESIGN of internal control framework		OPERATIONAL EFFECTIVENESS of internal controls	
	Findings from review	Design Opinion	Findings from review	Effectiveness Opinion
Substantial 	Appropriate procedures and controls in place to mitigate the key risks.	There is a sound system of internal control designed to achieve system objectives.	No, or only minor, exceptions found in testing of the procedures and controls.	The controls that are in place are being consistently applied.
Moderate 	In the main there are appropriate procedures and controls in place to mitigate the key risks reviewed albeit with some that are not fully effective.	Generally a sound system of internal control designed to achieve system objectives with some exceptions.	A small number of exceptions found in testing of the procedures and controls.	Evidence of non compliance with some controls, that may put some of the system objectives at risk.
Limited 	A number of significant gaps identified in the procedures and controls in key areas. Where practical, efforts should be made to address in-year.	System of internal controls is weakened with system objectives at risk of not being achieved.	A number of reoccurring exceptions found in testing of the procedures and controls. Where practical, efforts should be made to address in-year.	Non-compliance with key procedures and controls places the system objectives at risk.
No 	For all risk areas there are significant gaps in the procedures and controls. Failure to address in-year affects the quality of the organisation's overall internal control framework.	Poor system of internal control.	Due to absence of effective controls and procedures, no reliance can be placed on their operation. Failure to address in-year affects the quality of the organisation's overall internal control framework.	Non compliance and/or compliance with inadequate controls.

Recommendation Significance	
High 	A weakness where there is substantial risk of loss, fraud, impropriety, poor value for money, or failure to achieve organisational objectives. Such risk could lead to an adverse impact on the business. Remedial action must be taken urgently.
Medium 	A weakness in control which, although not fundamental, relates to shortcomings which expose individual business systems to a less immediate level of threatening risk or poor value for money. Such a risk could impact on operational objectives and should be of concern to senior management and requires prompt specific action.
Low 	Areas that individually have no significant impact, but where management would benefit from improved controls and/or have the opportunity to achieve greater effectiveness and/or efficiency.

www.bdo.co.uk

Ayrshire College (Paper 6)

Audit Committee

19 March 2019

Subject:	2018-19 Internal Audit Rolling Internal Audit Action Plan at 10 March 2019
Purpose:	To provide Members with an update on the Rolling Internal Audit Action Plan as at 10 March 2019
Recommendation:	The Audit Committee notes the content of this paper.

---

1. Background

The rolling Internal Audit Action Plan was last presented to the Audit Committee at its meeting on 27 November 2018. The rolling action plan is updated on an exceptions basis for actions approved by the Audit Committee which are now beyond their agreed completion dates.

2. Current Situation

All outstanding internal audit action points from our previous internal audits were completed meaning all recommendations made by Scott-Moncreiff have been cleared.

The Rolling Internal Audit Action Plan for 2018-19 onwards will cover any future audit recommendations made by our current internal auditors (BDO), once the audit reports and proposed management responses have been approved by the Audit Committee. The three year audit plan approved by the Audit Committee on 18 June 2018 commenced on 22 October with an audit of the College's risk management arrangements.

The first three internal audit reports prepared by BDO are presented to the March Audit Committee. Management is working to complete all the proposed management responses within the timescales outlined. Following approval of the reports progress against these audit recommendations will be formally reported to the Audit Committee.

3. Proposals

No further proposals are contained in this report.

4. Consultation

No formal consultation is required to be completed given the subject matter of this report.

5. Resource Implications

There are no resource implications to be noted in this paper.

6. Risks

An effective and challenging Internal Audit service is a key element in the management of risk within the College.

7. Equality Impact Assessment

An impact assessment is not applicable to this paper given the subject matter.

8. Conclusion

The Audit Committee notes the content of this paper.

Michael Breen
Vice Principal, Finance and Skills
10 March 2019

(James Thomson, Director of Finance and Student Funding)

Publication

This paper will be published on the College website.