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
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 Founding Council at the Board Strategy Day on 20 February 2017.

SCHEDULE OF BOARD AND COMMITTEE MEETINGS 2017-2018

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

Ayrshire College

Internal Audit Report 2017/18

Business Continuity Planning

October 2017

Scott-Moncrieff
business advisers and accountants

Ayrshire College

Internal Audit Report 2017/18

Business Continuity Planning

Audit Sponsor	*Key Contacts*	*Audit team*
Michael Breen, Vice Principal of Finance & Skills	*James Thomson, Director of Finance & Student Funding*	*Paul Kelly, IT Audit Director* *Scott Bannerman, IT Auditor* *Rachel Wilson, IT Auditor*

Executive Summary

Conclusion

Ayrshire College's refreshed Business Continuity plan was approved by the Audit Committee in June 2017. The development of the plan was led by the Vice Principal of Finance & Skills along with the former Director of ICT & MIS, and based on a previous BCP approved in November 2014.

The College has undertaken significant work in developing the current business continuity plan (BCP). Our audit work has identified that there are opportunities to improve the current BCP. In developing the current BCP, a Business Impact Analysis (BIA) was not conducted. This is an important process in establishing key services/critical activities as well as recovery strategies.

As part of the next review of the BCP, the College should perform a BIA which can be used to confirm whether there are any gaps within the current BCP. Similarly that review process should also be used to assess recovery strategies within the plan. The focus of this review should be to gain assurance that the recovery strategies are appropriately designed around the return of identified key services and include details of supporting activities and resources.

To assist with this review, the College's BCP would benefit from understanding, calculating and documenting recovery time objectives, recovery point objectives and maximum tolerable period of disruption for each key service/process as this supports the development of optimal recovery strategies and allows recovery allocation priorities to be set.

It will also be important for the College to develop and implement a risk-based programme of testing to allow assurance to be gained that they are capable of supporting the response to a business disruption.

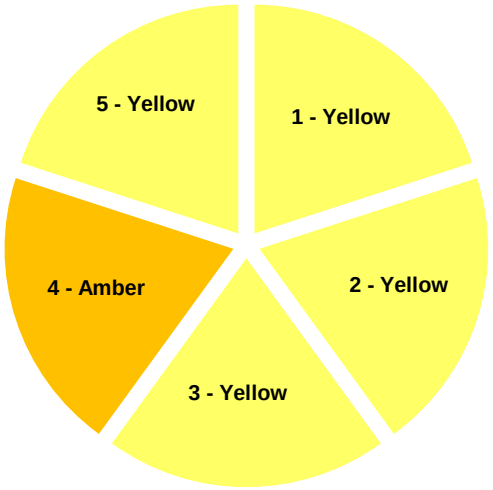
Background and scope

The ability to respond to unexpected events and provide continuity of service is critical to the organisation and it is essential that formal plans and procedures exist to support it in the event of a disaster.

The effectiveness of these plans requires a structured and methodical approach to identifying critical business processes, contingent resources, and optimal recovery strategies as well as robust maintenance and test processes

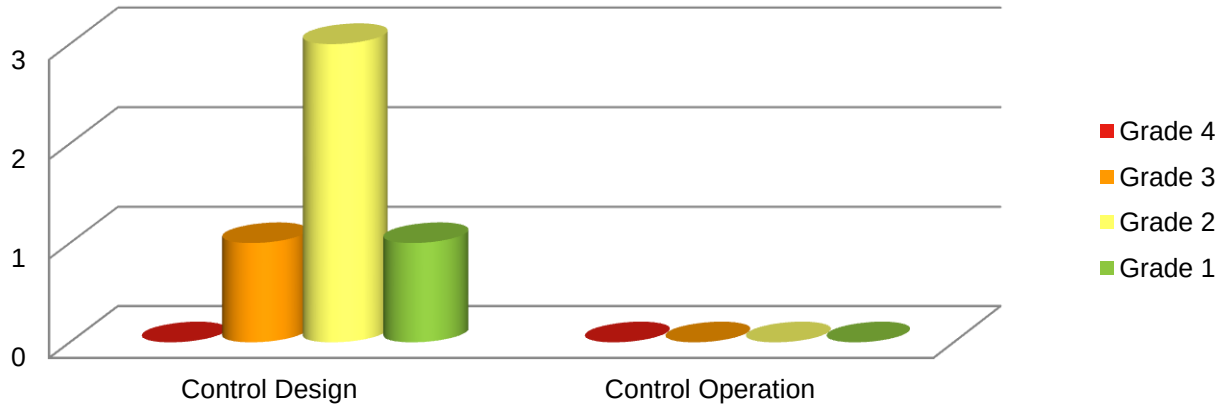
This review considered the extent to which the College has implemented an effective Business Continuity Management (BCM) framework and ensured appropriate testing of plans.

Control assessment



- A BCM framework, including policy and governance arrangements, has been implemented with roles and responsibilities assigned.
- Business Continuity Plans demonstrate a comprehensive understanding of the organisation, identifying the key services, as well as the critical activities that support them.
- Comprehensive and robust plans have been developed to manage the initial response to an incident and ensure the continuity of critical activities can be maintained.
- Effective processes exist to ensure business continuity arrangements are kept up-to-date and plans are regularly exercised and reviewed.
- Business continuity has strong support from senior management. There is good awareness of business continuity issues.

Improvement actions by type and priority



Five improvement actions have been identified from this review, all of which relate to the design of controls themselves. See Appendix A for definitions of colour coding.

Key findings

Good practice

We have gained assurance that Ayrshire College's procedures reflect good practice in the following area:

- IT has been heavily involved in the creation of the plan and has detailed disaster recovery procedures in place.

Areas for improvement

We have identified three areas for improvement which, if addressed, would strengthen the college's control framework. These include:

- It is intended that business continuity policy requirements are contained within the BCP. Although there is reference to governance groups and roles and responsibilities, the policy requirements associated with these areas is not set out in detail.

- As part of the development of a future BCP, it is recommended that a Business Impact Analysis (BIA) is performed. ISO22301 (the international business continuity standard) highlights this an important part of the development of BCPs and involves identification of business critical services and understanding the impact of disaster scenarios on them. This process is also critical in informing the development of recovery strategies and development of plans. By conducting a BIA this will allow the College to confirm whether there are any gaps within the current BCP. Similarly that review process should also be used to assess recovery strategies within the plan. The focus of this review should be to gain assurance that the recovery strategies are appropriately designed around the return of identified key services and include details of supporting activities and resources.

- To assist with this review, the College's BCP would benefit from understanding, calculating and documenting the MTPD, RTOs and RPOs for each key service/process as this supports the development of optimal recovery strategies and allows recovery allocation priorities to be set

- A formal programme of testing has not yet been developed by the College to confirm that the plans are capable of supporting the response to a business disruption.

These are further discussed in the Management Action Plan below.

Impact on risk register

The college's corporate risk register included the following risk relevant to this review:

- FIN4 - Failure of key ICT infrastructure and College business systems to support Ayrshire College services (Current Position = 9 (Likelihood 3, Impact 3)).

Our audit work has identified three areas for improvement in relation to business continuity arrangements that may affect the likelihood of this risk occurring. We would recommend that management reconsider the current rating of this risk in light of the issues raised in this report.

Acknowledgements

We would like to thank all staff consulted during this review for their assistance and co-operation.

Management Action Plan

Control Objective 1: A BCM framework, including policy and governance arrangements, has been implemented with roles and responsibilities assigned.

Yellow

1.1 Business Continuity Management Framework

The College does not have a formal Business Continuity Management (BCM) policy. A number of the elements of a Business Continuity Policy are included to some extent in the Business Continuity Plan although the policy requirements of them could be more clearly stated. For example, the governance provided through the Business Continuity and Risk Group and roles and responsibilities for Business Continuity within the College are not clearly defined.

We also noted that a Business Continuity and Risk Group has been formed but had not yet met at the time of our audit fieldwork. The first meeting took place on 7 November 2017. The Group comprises a wide representation of College management. The Group members have roles and responsibilities for the major functions and services contained within the BCP.

Risk

There is a risk that, if business continuity policy requirements are not well defined, this could result in a lack of clarity on roles and responsibilities within the College. There is also a risk that there is ineffective oversight of business continuity arrangements if robust governance arrangements are not in place.

Recommendation

We recommend that the current BCP is updated to include more specific details on business continuity policy requirements, particularly in relation to governance arrangements and roles and responsibilities.

We recommend that the Business Continuity and Risk Group has responsibility for oversight of the policy development and implementation.

Management Action

Grade 1 (Design)

Agreed.

Action owner: Director of Finance & Student Funding **Due date:** 30 September 2018

Control Objective 2: Business Continuity Plans demonstrate a comprehensive understanding of the organisation, identifying the key services, as well as the critical activities that support them.

Yellow

2.1 Business Impact Analysis (BIA)

In conducting our audit work, we established that the College had undertaken significant work in establishing the current Business Continuity Plan. As part of producing the BCP, a risk assessment was performed across all business functions of the College. This assessment set out, at a function level, the risk associated with a series of pre-defined disaster scenarios/impacts e.g. flooding (internal and external), pandemic flu, loss of various utilities etc.

As part of the development of the current BCP, a Business Impact Analysis (BIA) was not completed. The purpose of a BIA is to identify and document key services and critical activities along with their supporting activities, systems and resources. This is typically performed for each critical business process within the organisation where there is a requirement to have a specific BCP. Conducting the BIA by using a standard approach will allow the College to assess whether the current BCP addresses all key services and critical activities as well as provide the opportunity to review and revisit the risk assessment that has been performed.

Risk

Without conducting a BIA there is a risk that the current recovery plans may not adequately support the response to a business disruption.

Recommendation

As part of the next planned update of the BCP, we recommend that management undertakes a Business Impact Analysis across all College directorates. The results of the BIA, along with the lessons learned/actions from testing of plans, should be used to identify whether there are any gaps in the current BCP. For example, have all key services/critical activities been addressed, are resources required to support recovery correctly defined, has the impact of a disaster been fully identified etc.

We have provided details in Appendix B of a suggested process to be followed when undertaking a BIA.

Management Action

Grade 2 (Design)

Agreed.

Action owner: Director of Finance & Student Funding **Due date:** 30 September 2018

Control Objective 3: Comprehensive and robust plans have been developed to manage the initial response to an incident and ensure the continuity of critical activities can be maintained.

Yellow

3.1 Recovery Strategies and Plans

Our audit work identified that the recovery strategies detailed within the current plans may not be aligned to critical business processes as they have not been derived from the output of a BIA. (MAP section 2.1).

Our audit work identified that there is the potential to enhance current recovery plans by considering three business continuity metrics: recovery time objectives (RTOs), recovery point objectives (RPOs) and maximum tolerable period of disruption (MTPD).

- RTO is the period of time following an incident within which a product, service or an activity must be resumed, or resources must be recovered.
- RPO is the point to which information used by an activity must be restored to enable the activity to operate on resumption.
- MTPD is the time it would take for adverse impacts, which might arise as a result of not providing a product/service or performing an activity, to become unacceptable.

We did note that the current template used for individual recovery plans contains a section in which 'Recovery Timeframe' is to be recorded. This is defined as *"how quickly must this function be recovered to avoid lasting damage"*. Based on the bullet points above, this definition aligns most closely to MTPD. From reviewing the BCP, some departments have not clearly specified (in hours/days/weeks) what their recovery timescales are.

The College's BCP would be enhanced by understanding, calculating and documenting these metrics. Doing so will result in more informed recovery strategies to be designed and will also support the College in establishing recovery priorities. They also help to inform discussions with areas such as ICT in determining the priority in which ICT services/systems are to be restored in the event of a business disruption.

We also noted that, as the BCP is based around generic scenarios e.g. loss of access to accommodation, they do not provide specific details on how to recover those activities affected by a business disruption nor do they define the resource requirements to support this.

Risk

If recovery strategies are not aligned to key business processes, there is a risk that the BCP will not provide appropriate support to a user in the event of disruption.

In the absence of defined RTOs and RPOs, departments may not be able to identify when key services/ processes have to be restored. Where the MTPD has not been documented, there is a risk - particularly in the event of a major incident – that the order of recovery is not aligned to the associated risk in the timing of recovery.

Recommendation

As part of the review recommended in MAP2.1, we recommend that the College reviews its recovery strategies to confirm that they are aligned to key services/critical activities. The focus of this review should be to gain

assurance that they the recovery strategies are appropriately designed around the return of identified key services and include details of supporting activities and resources.

To assist with this review, the College's BCP would benefit from understanding, calculating and documenting the MTPD, RTOs and RPOs for each key service/process as this supports the development of optimal recovery strategies and allows recovery allocation priorities to be set. In addition, MTPD, RTO and RPO information should be cross-checked with ICT to confirm whether resilience and recovery arrangements are aligned to recovery strategies and recovery interdependencies i.e. is the current technology infrastructure/configuration capable of meeting recovery requirements?

We recommend that recovery procedures within plans are structured in a clear, concise and logical manner and that actual recovery steps form the body of plan documents. These should specify – ideally in the format of a step-by-step guide - the procedures to be followed as part of the immediate and ongoing response to an incident.

Management Action

Grade 2 (Design)

Agreed.

Action owner: Director of Finance & Student Funding **Due date:** 30 September 2018

Control Objective 4: Effective processes exist to ensure business continuity arrangements are kept up-to-date and plans are regularly exercised and reviewed.

Amber

4.1 Formal Programme of Testing

A formal programme of BCP testing has not yet been developed. We were informed that the plan provided a useful aide in helping enact incident response measures in the past however we noted that the output/lessons learned from such incidents were not documented.

Risk

Without developing and implementing a formal programme of testing, there is the risk that appropriate levels of testing are not undertaken to establish the ability of the BCP to support an effective and efficient response to a business disruption.

Recommendation

We recommend that, once all BCPs have been developed and approved, management introduce a risk-based programme of testing for BCPs. This should include a range of tests, including live testing, and simulations of different scenarios. Testing must be targeted at areas of the College that are likely to be most susceptible to an incident and/or would suffer the most adverse consequences. This may include full or partial of loss of access to a campus, full or partial loss of ICT network and/or systems, loss of staff etc.

Live testing seeks to recreate a realistic threat to business continuity. These tests should, where possible, closely simulate an actual incident to provide assurance that BCPs will aid the return of disrupted business critical services.

The outcomes of these tests should be formally documented and identify 'lessons learned'. Plans should be confirmed as appropriate following completion of tests.

Management Action

Grade 3 (Design)

Agreed. This has already been identified as a key action for the College by the Business Continuity and Risk Group.

Action owner: Director of Finance & Student Funding **Due date:** 31 March 2018

Control Objective 5: Business continuity has strong support from senior management. There is good awareness of business continuity issues.

Yellow

5.1 Employee Awareness and Training

Our audit found that there is a need to raise the profile of BCP across the various stakeholders groups within the College. We noted that there was limited involvement of senior management in the process of developing the current BCP. Management was asked to complete risk assessment and submit this to the (former) Director of IT. There was no subsequent involvement in the production of the current plan.

It was identified that there has yet to be any general awareness training provided for staff in relation to BC. We do note however that the establishment of the BCP Group is intended to provide a regular focus on BCP activity.

Risk

If a positive business continuity culture is not embedded within the College, there is the risk that staff members will not have the required level of knowledge and will not fully understand their responsibilities effectively should BCPs be invoked.

Recommendation

We recommend that there is active promotion by senior management to emphasise the importance of business continuity. This could be in the form of emails campaigns or staff newsletters.

In addition to this, we recommend that formal business continuity training is developed and rolled out to staff. This may be in the form of an eLearning module which staff are required to complete.

Management Action

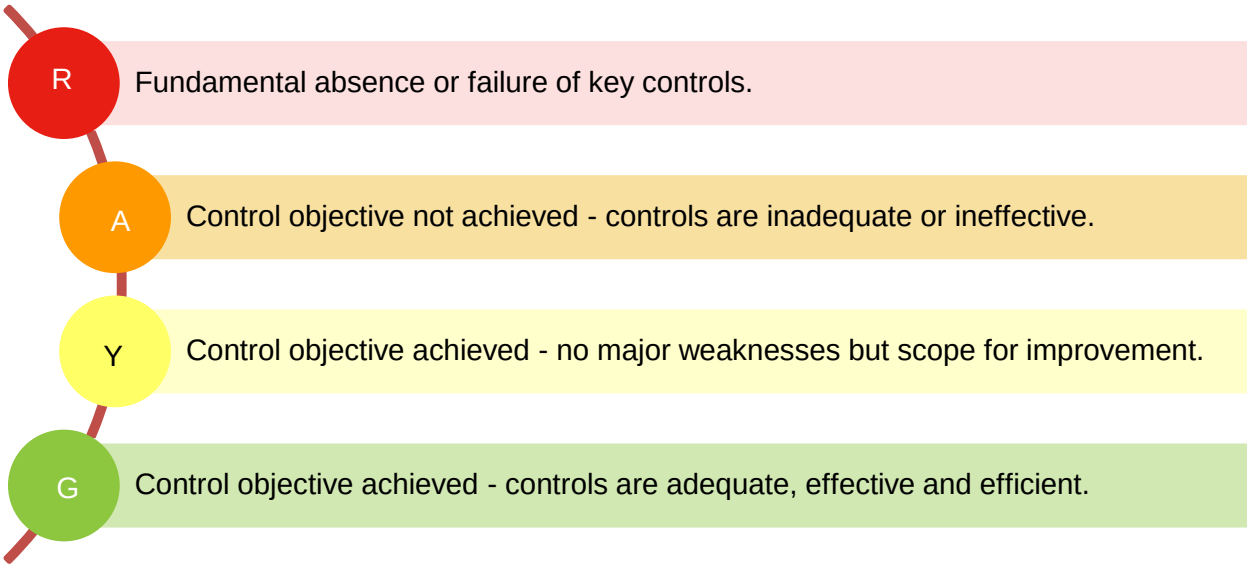
Grade 2 (Design)

Agreed. Training and raising employee awareness will be part of the College's ongoing business continuity processes.

Action owner: Director of Finance & Student Funding **Due date:** 31 March 2018

Appendix A – Definitions

Control assessments



Management action grades

4	•Very high risk exposure - major concerns requiring immediate senior attention that create fundamental risks within the organisation.
3	•High risk exposure - absence / failure of key controls that create significant risks within the organisation.
2	•Moderate risk exposure - controls are not working effectively and efficiently and may create moderate risks within the organisation.
1	•Limited risk exposure - controls are working effectively, but could be strengthened to prevent the creation of minor risks or address general house-keeping issues.

Appendix B

Business Impact Analysis (BIA)

Management should seek to develop an understanding of the organisation through the identification of its key services and the activities and resources that support them. By undertaking this process, it confirms that the approach to business continuity planning has been fundamentally aligned to the organisation's objectives, obligations and statutory duties.

There are a number of sequential steps in conducting a comprehensive BIA. These include:

- Identify all business critical functions within the organisation i.e. those which are implicit in the delivery of the organisations core mission;
- For each business critical function identify all the key services delivered by each function;
- Map the workflow of identified key services (potentially using tools such as swim lane diagrams) to ensure all supporting activities and resources are not overlooked.
- Assess (over time) the impact to the organisation in the event that a key service was to be disrupted. Consider the impact to functions, staff, students, reputation, the environment, financial viability etc.
- Determine the requirements (staff, facilities, and equipment/technology, information and suppliers) to partially/fully resume each key service.
- Evaluate the most likely threats that would prevent each key service being conducted. These typically include loss of staff, loss of premises, loss of equipment, loss of information.

Ayrshire College

Internal Audit Report 2017/18

Risk Management

January 2018

Scott-Moncrieff
business advisers and accountants

Ayrshire College

Internal Audit Report 2017/18

Risk Management

Audit Sponsor	*Key Contacts*	*Audit team*
Michael Breen, Vice Principal, Finance and Skills	*James Thomson, Director of Finance and Student Funding*	*Chris Brown, Partner* *Elizabeth Young, Director* *Andrew Diffin, Internal Auditor*

Executive Summary

Conclusion

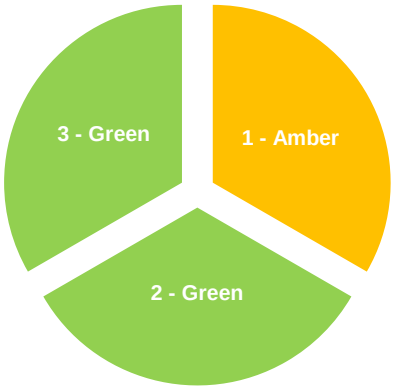
Ayrshire College has developed and implemented a robust framework for the management of strategic risks. The recommendation from our May 2014 report that the framework be extended to include operational risks remains outstanding however. We have identified a small number of other opportunities to strengthen the framework as presently implemented and set out some issues for consideration as the College further develops its risk maturity.

Background and scope

The Scottish Public Finance Manual states that 'Each public sector organisation's internal control systems should include embedded arrangements for identifying, assessing and managing risks'. Risk management is a process effected by the senior management team to identify potential future events and manage the associated risks, thereby providing reasonable assurance that the organisation will achieve its objectives.

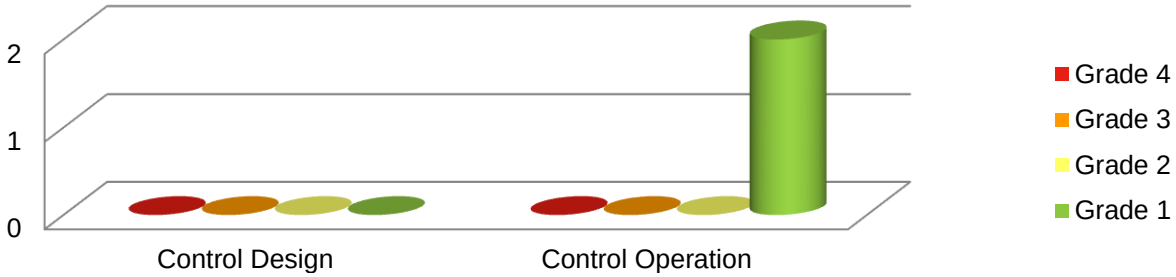
In accordance with the 2017/18 Internal Audit Plan, we have performed a review of risk management to confirm new arrangements are embedded and operating effectively. This included an assessment of the College's current level of risk maturity.

Control assessment



- 1. There is a defined and consistent approach for the accurate and timely identification and evaluation of risks
- 2. The Board has set the College's risk appetite and management are using this to inform decision making
- 3. There is an effective process for escalating and reporting risks to senior management and the Board

Improvement actions by type and priority



Two improvement actions have been identified from this review, both of which relate to the operation of existing controls rather than weaknesses in their design. See Appendix C for definitions of colour coding.

Key findings

Good practice

The College has made significant progress in developing its risk maturity since our previous review in 2014. We have gained assurance that the College's revised policies and procedures reflect good practice in a number of areas:

- The College's Strategic Plan 2017-20 has clearly defined objectives, which supports the effective identification of strategic risks. The College has developed and implemented a robust framework for the management of these risks.
- The risk framework includes a formal, quantified structure for risk scoring and assessing risk appetite, which provides a sound basis on which to assess the adequacy of controls. The College applies this framework to both strategic risks and any significant projects undertaken.
- There is a clear structure of responsibility and oversight, with the responsibilities of executive management, the Audit Committee, and the Board of Management defined in policy. Individuals with a role in the risk management process have received training to enable them to fulfil their responsibilities effectively.

Areas for improvement

We have set out two recommendations that, if implemented, will further develop the College's risk maturity by embedding its risk management framework at an operational level. These include:

- Expanding the scope of the risk management framework to encompass operational risks, by developing, implementing, and embedding risk registers at an operational level. This would enable management and the Board to gain greater assurance that all risks to the achievement of the College's objectives have been identified, and are being satisfactorily controlled.
- Reviewing and updating the Risk Management Policy to address some minor inconsistencies between current practice and the Policy as written.

These are further discussed in the Management Action Plan below.

Impact on risk register

This review is not linked to a specific risk from the Corporate Risk Register but has a relevance to the risk management framework as a whole.

Acknowledgements

We would like to thank all staff consulted during this review for their assistance and co-operation.

Management Action Plan

Control Objective 1: There is a defined and consistent approach for the accurate and timely identification and evaluation of risks.

1.1 Operational Risk Registers

The College has made significant progress developing and implementing a risk management framework at the strategic level, however the framework does not presently capture operational objectives and risks.

Our May 2014 review of risk management recommended "that operational risk registers are established to ensure that operational level risks are identified and addressed", and this remains an outstanding action on the College's Internal Audit Action Tracker. We have applied the grading from that previous review however have not raised a further recommendation. We will continue to track the College's progress in implementing this action through our regular follow up review.

Implementing operational risk registers will contribute to progressing the College's risk maturity from "Risk Defined" to "Risk Managed" according to the Chartered Institute of Internal Auditors (IIA) Risk Maturity Scale. Our assessment of the College's current risk maturity is set out in Appendix A.

The College has begun to take steps to implement this recommendation, and so in carrying out this review we have considered potential issues that may arise in applying the College's existing risk management framework at the operational level. We have set out three advisory points that we recommend that the College should consider and address while implementing and embedding operational risk registers. These are set out in Appendix B.

1.2 Review of Risk Management Policy

The current version of the Risk Management Policy bears a review date of December 2017, however no review has yet been carried out. We understand that review of the policy was deferred pending the outcome of this audit and further progress in relation to the implementation of operational risk registers, however this decision was not formally recorded.

Risk

If the Risk Management policy is not updated according to its review schedule, there is a risk that assumptions which are no longer appropriate are carried forward, leading to inappropriate risk management decisions and adverse risks materialising.

Recommendation

The College should review the policy in line with the established timetable, or formally record decisions to vary the timetable if it is deemed to be inappropriate. The College should consider when the policy should be reviewed in future, as amendments or additions may be required as the College implements its plans to introduce and embed risk management at an operational level.

Management Action

Grade 1 (Operation)

This will be included within the revised Risk Management Policy.

Action owner: Director of Finance and Student Funding **Due date:** 30 June 2018

Control Objective 2: The Board has set the organisation's risk appetite and management are using this to inform decision-making.

Green

2.1 Risk Appetite Scoring System

The Risk Management Policy incorporates a system of risk scoring, including guidance as to how this should be applied when defining risk appetite.

In practice the College applies a slightly different scoring system to statements of risk appetite in the risk register itself. The system used in the Risk Register consists of five categories, whereas the policy specifies only four. There is no significant inconsistency between the two, however the system applied within the risk register allows for greater precision.

Risk

There is a risk that the College's appetite towards certain risks may, in come cases, be overstated to a small degree, leading to failure to identify and implement adequate controls, resulting in the realisation of a risk outside the College's appetite.

Recommendation

The College should update the Risk Management Policy to reflect the risk appetite scoring system that is used in practice.

Management Action

Grade 1 (Operation)

The College decided to make no further minor amendments to the Policy until the corporate risk management approach was embedded within the College (i.e. until the approach had gone through at least one calendar cycle).

The risk appetite scoring system will be amended within the revised Risk Management Policy.

Action owner: Director of Finance and Student Funding **Due date:** 30 June 2018

Control Objective 3: There is an effective process for escalating risks and for reporting risks to senior management and the Board.

Green

No issues identified

Subject to the advisory recommendations set out in Appendix A, we have not identified any issues with the College's arrangements for oversight and reporting of the operation of the risk management framework in the areas where it has been implemented.

The Risk Management Policy assigns responsibility for overseeing the operation of the risk management framework to the Audit Committee, and sets out specific review and reporting duties. Extracts from the risk register are presented to each of the Board's sub-committees in line with their delegated remits. The risk register is reviewed in full by the Audit Committee on a quarterly basis in order to provide scrutiny and challenge to the Board sub-committees responsible for identifying and assessing risk. The Audit Committee receives assurance through internal and external audit reports, and provides an annual report to the Board setting out how its responsibilities have been discharged.

Appendix A – IIA Maturity Scale

We have used the Chartered Institute of Internal Auditors (IIA) Risk Maturity Scale to assess the risk maturity of the College. To inform our assessment we:

- discussed risk management arrangements with the Director of Finance and Student Funding; and
- undertook a detailed review of risk management documentation.

We assessed the College's risk maturity as falling between the "Risk Defined", and "Risk Managed" categories. Our assessment for each risk maturity process is highlighted in blue within the Risk Maturity Scale below. The Scale gives some indication of expected risk management behaviours should the College wish to progress towards being a "Risk Enabled" organisation. The implementation of the risk management recommendations contained within our report will assist the College in moving to the "Risk Managed" category, if desired.

	Risk Naïve	Risk Aware	Risk Defined	Risk Managed	Risk Enabled
Key Characteristics					
	No formal approach developed for risk management	Scattered silo based approach to risk management	Strategy and policies in place and communicated and risk appetite defined.	Enterprise approach to risk management developed and communicated	Risk management and internal controls fully embedded into the operations
Process					
The organisation's objectives are defined	Possibly	Yes - but may be no consistent approach	Yes	Yes	Yes
Management have been trained to understand what risks are, and their responsibility for them	No	Some limited training	Yes	Yes	Yes

:	Risk Naïve	Risk Aware	Risk Defined	Risk Managed	Risk Enabled
A scoring system for assessing risks has been defined	No	Unlikely, with no consistent approach defined	Yes	Yes	Yes
The risk appetite for the organisation has been defined in terms of the scoring system	No	No	Yes	Yes	Yes
Processes have been defined to determine risks, and these have been followed	No	Unlikely	Yes, but may not apply to the whole organisation	Yes	Yes
All risks have been collected into one list. Risks have been allocated to specific job titles	No	Some incomplete lists may exist	Yes, but may not apply to the whole organisation	Yes	Yes
All risks have been assessed in accordance with the defined scoring system	No	Some incomplete lists may exist	Yes, but may not apply to the whole organisation	Yes	Yes
Responses to the risks have been selected and implemented	No	Some responses identified	Yes, but may not apply to the whole organisation	Yes	Yes
Management have set up methods to monitor the proper operation of key processes, responses and action plans ('monitoring controls')	No	Some monitoring controls	Yes, but may not apply to the whole organisation	Yes	Yes
Risks are regularly reviewed by the organisation	No	Some risks were reviewed, but infrequently	Regularly reviewed, probably annually	Regularly reviewed, probably quarterly	Regular reviews, probably quarterly

	Risk Naïve	Risk Aware	Risk Defined	Risk Managed	Risk Enabled
Management report risks to directors where responses have not managed the risks to a level acceptable to the board	No	No	Yes, but may be no formal process	Yes	Yes
All significant new projects are routinely assessed for risk	No	No	Most projects	All projects	All projects
Responsibility for the determination, assessment, and management of risks is included in job descriptions	No	No	Limited	Most job descriptions	Yes
Management provide assurance on the effectiveness of their risk management	No	No	No	Some managers	Yes
Managers are assessed on their risk management performance	No	No	No	Some managers	Yes

Appendix B – Advisory Recommendations

The College is in the process of applying its risk management framework at an operational level. In carrying out this review, we have considered the application of the framework at the strategic level, but have also considered areas where the framework as presently designed and implemented may require modification or enhancement in order to be suitable for application at the operational level.

Ayrshire College has developed a strategic risk management approach that reflects good practice. As the College develops and implements operational risk registers it should ensure that this good practice is also reflected at an operational level. We have identified three areas where the College should give due consideration to help to ensure that the risk management framework is effective at all levels of the organisation.

A.1 – Risk Register Links to Objectives

The College has a number of approved planning documents, including the College Strategy, Outcome Agreement, and Curriculum Development Plan. These set out a variety of strategic and operational objectives.

Where operational objectives are set out in planning documents, operational risk registers should enable the College to gain assurance that risks to their achievement have been identified, assessed, and are being managed appropriately. Accordingly, we would advise that the operational risk registers should set out how identified risks and associated controls influence the College's ability to meet these objectives, i.

A.2 – Responsibilities and Accountability

At the level of the Board and Senior Management, individuals assume responsibility for risk management through their overall responsibility to contribute towards the achievement of the College's objectives. Within operational areas of the organisation, the responsibilities of particular individuals are unlikely to be as broadly defined. There is therefore a risk that individuals at an operational level are not made aware of their responsibilities in relation to risk management, or that performance appraisal does not take this into account.

We understand that the College will use a similar template for its operational risk registers as is used for the Strategic Risk Register. This template sets out the key staff responsible for the risk identified. The College should ensure these responsibilities are communicated effectively to the staff identified and that their risk management responsibilities are considered as part of their performance appraisal process.

A.3 – Assurance

The Audit Committee is responsible for overseeing the operation of the risk management framework, and providing assurance to the Board on the effectiveness of its operation. The Audit Committee carries out regular reviews of the risk register prior to approval by the Board, and annually reports to the Board on the discharge of its responsibilities.

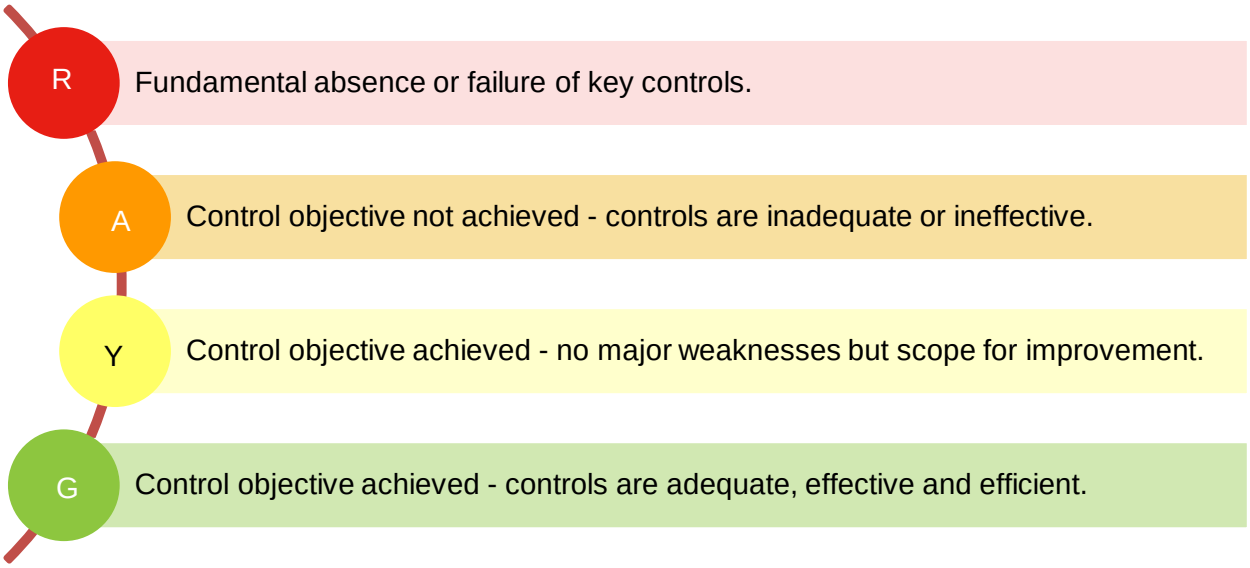
It is unlikely to be practical for the Audit Committee to carry out a similar level of review of operational risk registers, and the Risk Management Policy in its present form does not set out any alternative means for operational risk registers to be reviewed, and assurance provided to the Board with regards to the operation of controls.

The College should consider how the effectiveness of risk management arrangements at the operational level will be reviewed, and ensure that this provides the Audit Committee and Board with adequate assurance that

the arrangements are operating effectively. This should include outlining the process for escalating operational risks to the strategic risk register within the College's Risk Management Policy.

Appendix C – Definitions

Control assessments



Management action grades

4	•Very high risk exposure - major concerns requiring immediate senior attention that create fundamental risks within the organisation.
3	•High risk exposure - absence / failure of key controls that create significant risks within the organisation.
2	•Moderate risk exposure - controls are not working effectively and efficiently and may create moderate risks within the organisation.
1	•Limited risk exposure - controls are working effectively, but could be strengthened to prevent the creation of minor risks or address general house-keeping issues.

Ayrshire College

Internal Audit Progress Report

March 2018

Scott-Moncrieff
business advisers and accountants

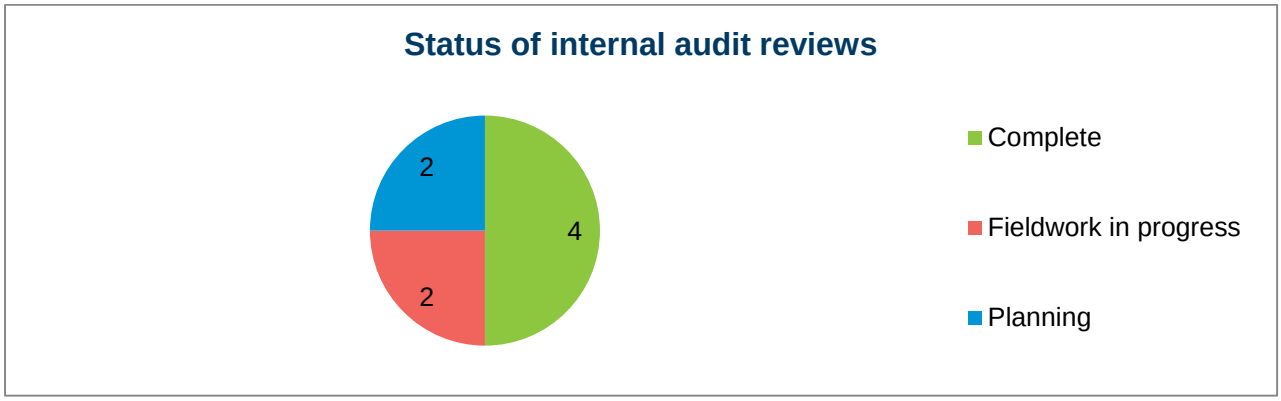
Ayrshire College

Internal Audit Progress Report

Summary of Progress

This paper provides the Audit Committee with a summary of internal audit activity since its last meeting and confirms the reviews planned for the coming quarter, identifying any changes to the original annual plan.

Progress against annual audit plan



We have completed two audits in the period to March 2018 – Risk Management and Business Continuity Planning. We have made progress in delivering the remaining 2017/18 audits and are on track to deliver the audit plan as agreed with management and the Audit Committee.

Appendix 1 sets out the status of the 2017/18 internal audit programme.

Plan for next quarter

We will present the following reports to the June 2018 audit committee:

- Key Financial Systems
- SFC Financial Returns – Resources and Cash Drawdowns
- Student Experience (Student Services)
- Estates Strategy

Action for Audit Committee

The Audit Committee is asked to note the contents of this report and to approve the plan for the next quarter. We also invite any comments on the format or content of this report. Contact details are as follows:

Chris Brown, Audit Partner	chris.brown@scott-moncrieff.com	0131 473 3500
Elizabeth Young, Director	elizabeth.young@scott-moncrieff.com	0141 567 4500

Appendix 1 – Progress against 2017/18 internal audit plan

Ref and Name of report	Audit Sponsor	Status	Quarter	Planned Audit C'ttee	Actual Audit C'ttee
A2. Risk management	Board Secretary	Complete	Q2	Mar 18	Mar 18
B1. Key Financial Systems	Director - Finance and Student Funding	Fieldwork in progress	Q2	Jun 18[1]	
B2. SFC Financial Returns – Resources and Cash Drawdowns	Director - Finance and Student Funding	Planning	Q3	Jun 18	
C1. Student Experience (Student Services)	Vice Principals	Fieldwork in progress	Q3	Jun 18	
D2. Estates Strategy	Vice Principal- College Estate & Facilities	Planning	Q3	Jun 18	
D3. Business Continuity Plan	Director – ICT and MIS	Complete	Q1	Mar 18	Mar 18
E1. Student Support Funds	Director - Finance and Student Funding	Complete	Q1	Dec 17	Dec 17
E2. Student Sums	Director - Finance and Student Funding	Complete	Q1	Dec 17	Dec 17
F1. Follow up	N/A	N/A	Q4	Sept 18	

Key:	

[1] Originally scheduled for March; however fieldwork was delayed at the request of management

Complete	Audit work complete and report has been agreed and finalised
Draft Report	A draft report has been issued
Fieldwork complete	The audit work is complete but the draft report has not yet been issued.
Fieldwork in progress	The audit work is in progress.
Planned	The scope and timing have been agreed with management
Planning	The scope of the audit has yet to be agreed with management

Ayrshire College (*Paper 4a)*

Audit Committee

20 March 2018

Subject:	Proposed Amendment to 2017-18 Internal Audit Plan
Purpose:	To seek Members approval for amending the agreed 2017-18 Internal Audit Plan.
Recommendation:	Members approve that the planned internal audit of the College's Estates Strategy is postponed until 2018-19.

---

1. Background

The Audit Committee approved the AY 2017-18 Internal Audit Plan on 15 June 2017. The Plan set out nine audits to be undertaken during 2017-18, this included a review of the College's Estates Strategy.

2. Current Situation

The College's estates activity is driven by operational need, statutory compliances, rolling replacement activity, compliance with all relevant legislation (e.g. the Equalities Act) and good sustainability practices. Estates activity has been funded by the College including the use of capital grants received from the Scottish Funding Council. Estates work has also been funded by Ayrshire College Foundation.

The College has undertaken a programme of significant estates work during AY 2016-17 and AY 2017-18. This includes new roofs and windows and the development of the new hospitality and tourism suite at the Ayr Campus, and the Learning and Resource Centre at Kilwinning.

The level of estates activity undertaken by the College has been recognised by the College's External Auditors (Mazars). In their Annual Report to the Board in December 2017 Mazars stated that "significant improvement works to the estate have been completed [by the College]". Mazars recommended that the College developed an Infrastructure Strategy to direct and formalise planned estates activity.

A draft Infrastructure Strategy was approved by the Business, Resources and Infrastructure Committee (BRIC) on 13 March 2018. The Strategy sets out the College's proposals for future estates, ICT and sustainability activity and will direct underlying estates operational work. The development of the draft Infrastructure Strategy was being actioned by management prior to the recommendation by Mazars.

The outline scope of the proposed Estates Strategy internal audit was to "review arrangements for estates management". The College has therefore received audit

guidance on this area through the review and recommendation of our External Auditors.

An internal audit of the College's estates activity would add more value when the Infrastructure Strategy has been approved. An internal audit at that time (i.e. during 2018-19) would provide the Audit Committee with assurance on the programme of estates activity undertaken to date and the extent to which this has reflected the key principles of the Infrastructure Strategy.

3. Proposals

We propose that the Internal Audit of the College's Estates Strategy is postponed until AY 2018-19.

4. Consultation

No formal consultation is required to be completed.

5. Resource Implications

No further resource implications require to be noted in this paper.

6. Risks

The College's Corporate Risk Register includes the risk that "facilities will be unavailable due to estate-related matters." This risk is mitigated by the significant estates work that has been undertaken by the College and the robust estates management controls in place. The risk will be further mitigated by the approval and implementation of the draft Infrastructure Strategy.

7. Equality Impact Assessment

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

8 Conclusion

Members approve that the planned internal audit of the College's Estates Strategy is postponed until 2018-19.

Donna Vallance
Vice Principal, Infrastructure and Skills
16 February 2018

[James Thomson, Director of Finance and Student Funding]

Publication

This paper will be published on the College website.

Ayrshire College (*Paper 5)*

Audit Committee Meeting

20 March 2018

Subject:	Rolling Internal Audit Action Plan at 21 February 2018
Purpose:	To provide an update on the Rolling Internal Audit Action Plan as at 31 January 2018
Recommendation:	Members note the contents of this report.

---

1. Background

The Rolling Internal Audit Action Plan was last presented to the Audit Committee at its meeting on 19 September 2017. The Plan has since been updated on an exceptions basis for actions which are now beyond their agreed completion dates.

2. Current Situation

2013-14 to 2016-17

Table 1 below lists all remaining points from the internal audits from 2013-14 to 2016-17.

Table 1

Ref	Audit Year	Audit Area	Points Raised	Actioned in Period	Remaining Points
1	2013-14	Risk Management	1	-	1
2	2014-15	Asset Management	1	-	1
3	2015-16	Key Financial Systems	1	-	1
4	2015-16	Health & Safety	3	3	-
5	2016-17	Corporate Governance	3	3	-
6	2016-17	Student Experience	5	5	-
		Total	**14**	**11**	**3**

We have set out below a summary of all remaining internal audit action points.

1. Risk Management

The action relates to the alignment of operational Risk Registers to the overall corporate Risk Register. The Business Continuity Plan Steering Group met on 30 January to develop draft operational risk registers. These risk registers are being prepared during February and will be presented to the Executive Management Team by 31 March 2018.

2. Asset Management

The item above relates to the development of a long term capital plan. A draft plan is being developed which will be aligned to curriculum requirements for 2017-20. This item will be completed during AY 2017-18.

3. Key Financial Systems

The point relates to updating the finance procedures manual. The Finance team had intended to finalise the procedures manual once the College receives the updated financial memorandum from SFC. The SFC has yet to confirm when the updated memorandum will be published. The revised procedures manual will be completed by 30 April 2018.

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

Members note the contents of this report.

Michael Breen
Vice Principal, Finance and Skills
21 February 2018

(James Thomson
Director of Finance and Student Funding)

Publication

This paper will be published on the College website.