

Board of Management Audit and Assurance Committee

Date of Meeting	Wednesday 13 May 2020
Paper No.	AAC4-C
Agenda Item	5.3.1
Subject of Paper	Internal Audit Report – Risk Management
FOISA Status	Disclosable
Primary Contact	Henderson Loggie
Date of production	May 2020
Action	For Discussion and Decision

Recommendations

The Committee is asked to consider and discuss the report and the management responses to the internal audit recommendations.

1. Purpose of report

The purpose of this review is to provide management and the Audit Committee with assurance on key controls relating to the curriculum and financial plans in place for City of Glasgow College and their alignment with the regional plan for Glasgow and the college student number targets.

2. Context and Discussion

This internal audit of Risk Management provides an outline of the objectives, scope, findings and graded recommendations as appropriate, together with management responses. This constitutes an action plan for improvement.

The Report includes a number of audit findings which are assessed and graded to denote the overall level of assurance that can be taken from the Report. The gradings are defined as follows:

Good	System meets control objectives.
Satisfactory	System meets control objectives with some weaknesses present.
Requires improvement	System has weaknesses that could prevent it achieving control objectives.
Unacceptable	System cannot meet control objectives.

3. Impact and implications

Refer to internal audit report.

City of Glasgow College

Risk Management

Internal Audit Report No: 2020/03

Draft issued: 13 March 2020

Final issued: 4 May 2020

LEVEL OF ASSURANCE

Good

Contents

Page No.

Section 1	Management Summary	
	<ul style="list-style-type: none"> • Overall Level of Assurance • Background • Scope, Objectives and Overall Findings • Audit Approach • Summary of Main Findings • Acknowledgements 	<p>1</p> <p>1</p> <p>2</p> <p>2</p> <p>3</p> <p>3</p>
Section 2	Main Findings and Action Plan	4 - 10

Level of Assurance

In addition to the grading of individual recommendations in the action plan, audit findings are assessed and graded on an overall basis to denote the level of assurance that can be taken from the report. Risk and materiality levels are considered in the assessment and grading process as well as the general quality of the procedures in place.

Gradings are defined as follows:

Good	System meets control objectives.
Satisfactory	System meets control objectives with some weaknesses present.
Requires improvement	System has weaknesses that could prevent it achieving control objectives.
Unacceptable	System cannot meet control objectives.

Action Grades

Priority 1	Issue subjecting the College to material risk and which requires to be brought to the attention of management and the Audit and Assurance Committee.
Priority 2	Issue subjecting the College to significant risk and which should be addressed by management.
Priority 3	Matters subjecting the College to minor risk or which, if addressed, will enhance efficiency and effectiveness.



Management Summary

Overall Level of Assurance

Good	System meets control objectives
-------------	---------------------------------

Background

As part of the Internal Audit programme at the College for 2019/20 we carried out a review of the College's risk management arrangements. The Audit Needs Assessment, completed in March 2017, identified this as an area where risk can arise and where Internal Audit can assist in providing assurances to the Board of Management and to the Principal that the related control environment is operating effectively, ensuring risk is maintained at an acceptable level.

The Scottish Public Finance Manual requires that public sector organisation's internal control systems should include embedded arrangements for identifying, assessing, and managing risks, with risk management closely linked to the business planning process. It requires that the Board makes a considered choice about its desired risk profile, taking account of its legal obligations, ministers' policy decisions, its business objectives, and public expectations of what it should deliver.

Good risk management includes a range of matters including:

- Creating a formal risk management framework, including identifying risk appetite;
- Risk identification;
- Risk assessment (likelihood and impact);
- Risk mitigation;
- Risk reporting and escalation; and
- Risk review and feedback.

Risk Management

Scope, Objectives and Overall Findings

The scope of this audit was to consider whether there were corporate procedures in place to adequately assess risk and minimise the possibility of unexpected and unplanned situations developing, which were in line with good practice.

The table on the below notes the objectives for this review and records the results:

Objective	Findings			
The objectives of this audit were to obtain reasonable assurance that systems are sufficient to ensure:		1	2	3
1. There is a process in place to provide reasonable assurance to the Board of Management and to the Principal in relation to the declaration on risk required for the financial statements	Good	0	0	0
2. The process in place applies good practice in risk management	Good	0	0	0
3. Key risks have been identified and are being appropriately controlled, mitigated, reported and discussed at appropriate levels of management and the Board of Management	Satisfactory	0	0	2
Overall Level of Assurance	Good	0	0	2
		System meets control objectives		

Audit Approach

We obtained and reviewed a copy of the College's Risk Management Policy, Procedure, Guidance and Risk Register and discussed the risk management arrangements in place with the College Secretary / Planning, Vice Principal Corporate Services and other key managers and staff. The College's risk management arrangements were then benchmarked against relevant good practice guidance. We also considered whether all relevant key risks had been identified and included on the Risk Register and ensured that these were being monitored and adequately reported on.

Risk Management

Summary of Main Findings

Strengths

- There is a robust risk management framework in place including: a Risk Management Policy; a Risk Management Procedure; Risk Management Guidance; Strategic Risk Register; Risk Management Action Plans; Operational Plans including sections for considering risks; and an escalation process to move risks from operational risks to the Strategic Risk Register; Audit and Assurance Committee review of the whole Risk Register; Board sub-committee review of specific risks on the risk register; and the Risk Register being provided to the Board;
- From our review of the risk management framework it exhibited most aspects of good practice; and
- There is a review of assurance provided by internal and external auditors which is summarised in the annual report of the Audit and Assurance Committee to the Board. In addition, senior managers provide assurance certificates to the Principal. This information is used to support the statement on adequacy of the risk management framework included in the College's annual report.

Opportunities for Improvement

- Given the parallel work to develop and implement the assurance framework, it was agreed that there would be benefit in providing additional staff training on this, which would provide the opportunity to introduce staff to elements of different risk management techniques.
- Not all significant projects were routinely assessed for risk

Acknowledgements

We would like to take this opportunity to thank the staff at the College who helped us during our audit visit.

Main Findings and Action Plan

Objective 1: There is a process in place to provide reasonable assurance to the Board of Management and to the Principal in relation to the declaration on risk required for the financial statements

The statement on risk in the 2018/19 annual report states '*The Board has a process for identifying, evaluating and managing the College's risks that has been in place for the year ending 31 July 2019, up to the date of approval of the annual report and accounts.*'

To support this statement there are a range of sources of assurance. Firstly, there are certificates of assurance, completed by 12 senior managers, which confirmed that they had reviewed the internal control arrangements in their area of responsibility and either confirmed that they had been working well and that there were no significant matters arising that needed to be raised in providing assurance to the Accountable Officer, or highlighting any significant matters that needed to be raised.

Secondly, the annual report of the Audit and Assurance Committee to the Board included information on a range of assurance sources, including internal audit and external audit, and outlined other relevant areas considered during the year (such as data protection, business continuity, development opportunities, authority limits and fraud).

In addition to the above, there were a range of other sources of assurance, such as the annual report of the external auditors and reports provided by external bodies (such as Education Scotland).

We consider that the process in place provides adequate assurance to the Board of Management and to the Principal in relation to the declaration on risk required for the financial statements.

We noted that the Board have approved the introduction of an assurance framework, supported by an assurance map. As part of this audit we discussed examples of assurance maps with the College Secretary / Planning and provided them with information on how this might be implemented in practice. A draft Assurance Framework was presented to the Audit and Assurance Committee on 19 February 2020.

Risk Management

Objective 2: The process in place applies good practice in risk management

We completed a risk management checklist with the College Secretary / Planning and from exercise we confirmed that the College applied most aspects of good practice. A small number of areas on the checklist were not embedded within the current College risk management arrangements. However, in discussion with management it was agreed that the effort involved in implementing these actions exceeded the likely benefits which would accrue.

Risk Management

Objective 3: Key risks have been identified and are being appropriately controlled, mitigated, reported and discussed at appropriate levels of management and the Board of Management

Risk Identification

We reviewed the Risk Register against peer College risk registers and did not identify any risks recorded on those risk registers that we considered should be reflected on the College's Risk Register.

Risk Mitigation and Reporting

We reviewed the College's Risk Register and noted a number of opportunities for refinement to the existing format. These were discussed with the College Secretary / Planning who advised that he would consider these suggestions before taking a view on whether changes were required to the existing format of the Risk Register.

As part of this audit we met with six managers from across the College to establish their knowledge of the College's risk management process; to explore the main risks they considered their area faced; and to consider whether there were appropriate controls in place to mitigate these risks. From these discussions a small number of issues were noted which the staff interviewed confirmed would be addressed by implementing additional controls.

We reviewed the Risk Register and associated Risk Management Action Plans (RMAs) and consider that the mitigating actions recorded were reasonable.

We also reviewed the reporting on risk to the Senior Management Team, Audit and Assurance Committee and Board and consider that the format of this reporting was appropriate.

Project Risk Management

A number of staff interviewed considered that there would be benefit in adopting a formal College project management methodology. We discussed this with the College Secretary / Planning who took the view that there would be limited benefit arising from the introduction of a standard project management methodology across the College and as a result no specific recommendation has been raised regarding this point.

One example of a significant project is the Taught Degree Awarding Powers (TDAP) project. As part of the audit we discussed this project with the full-time TDAP Director (Project Manager). We note that this project utilised a suite of standard project management documents and tools, including a risk register, to manage project risk. We noted that this project was on hold at the time of audit fieldwork in March 2020. It was noted that communications for the project were not being undertaken in line with the communications plan put in place by the TDAP Director. As a result of the issues encountered, the Project Manager had escalated the matter to the Depute Principal and COO who took the decision to cancel the Project Implementation Board meeting in November 2019. This was then further escalated to the Principal, Project Board, and Audit and Assurance Committee and this has now been recorded on the College's Strategic Risk Register. Plans have now been developed on how to restart the project. We consider that this is a good example of risk management in practice, with risks being identified and escalated upwards to allow greater oversight and agreement of an approach to addressing risks to project delivery going forward.

Risk Management

Objective 3: Key risks have been identified and are being appropriately controlled, mitigated, reported, and discussed at appropriate levels of management and the Board of Management (Continued)

Observation	Risk	Recommendation	Management Response		
<p>Assurance Map and Risk Management Training In order to ensure that staff embed risk management into their day to day operations (rather than treating risk management as a 'tick box' exercise) it is important to make sure that staff are appropriately trained in how to apply the agreed risk management process. A number of the staff members interviewed expressed the view that there would be benefit in providing additional risk management training. However, the College Secretary / Planning felt that this may be viewed by some members of staff as an additional burden and that accordingly this may not receive the required buy-in from staff. However, given the parallel work to develop and implement the assurance framework it was agreed that there would be benefit in providing additional staff training on this aspect, which would provide the opportunity to introduce staff to elements of different risk management techniques.</p>	<p>Staff may be aware of the risk management framework but may not be aware of risk management techniques in order to apply good practice in risk management</p>	<p>R1 The SMT should give consideration to how the new College assurance map will be rolled out, which should include some elements of staff training on risk management techniques. (Training may require to be delivered online in the short/medium term).</p>	<p>Agreed.</p> <p>To be actioned by: P Clark, College Secretary/Planning and SMT</p> <p>No later than: 31 October 2020</p>		
			<table border="1"> <tr> <td>Grade</td> <td>3</td> </tr> </table>	Grade	3
Grade	3				

Risk Management

Objective 3: Key risks have been identified and are being appropriately controlled, mitigated, reported and discussed at appropriate levels of management and the Board of Management (Continued)

Observation	Risk	Recommendation	Management Response	
<p>Project Risk We assessed the College's risk maturity against a risk maturity framework (see below). From this exercise it was identified that not all significant projects were routinely assessed for risk, and the College Secretary / Planning concurred with the view that there would be benefit in doing so. It was agreed that that this could be achieved by building this into the standard template for SMT papers, as all significant projects are routinely considered by SMT before proceeding.</p>	<p>Projects may not be assessed for risk, leading to the increased potential for project failure with the accompanying reputational damage.</p>	<p>R2 The standard template used for SMT papers should be adapted to incorporate a section to identify risks associate with significant projects. This template should include a risk table with standard headings (such as governance, stakeholders, finance) to be used as an aide memoire to help identify significant project risks, with supporting narrative to be provided around the impact and likelihood of the significant project risks identified.</p>	<p>Agreed.</p> <p>To be actioned by: P Clark, College Secretary/Planning</p> <p>No later than: 30 June 2020</p>	
			Grade	3

Risk Management

Other: Risk Maturity Framework Assessment

The College was assessed against the risk management maturity framework set out on the following page against the following five risk rankings:

- Enabled
- Managed
- Defined
- Aware
- Naïve

The results of our assessment was:

Risk maturity area	Risk assessment	Comments
Risk Governance	Defined	Risk management is not fully embedded in the College, and managers are not trained in risk techniques. This is covered by R1 above.
Risk Identification and Assessment	Defined	Not all significant projects are routinely assessed for risk. This is covered by R2 above.
Risk Mitigation and Treatment	Managed	A move to the higher 'enabled' category would require a more in-depth review of mitigation techniques (including assurance over the risks being effective). This will be partly covered by the introduction of the College's new assurance map.
Risk Reporting and Review	Managed	We found there was not consistent reporting of project risks. This is covered by R2 above.
Continuous Improvement	Managed	Management assurance on the effectiveness of risk management was not in place. This will be partly covered by the introduction of the College's new assurance map.

Risk Management

	Risk Governance	Risk Identification and Assessment	Risk Mitigation and Treatment	Risk Reporting and Review	Continuous Improvement
Enabled	Risk management and internal control is fully embedded into operations. All parties play their part and have a share of accountability for managing risk in line with their responsibility for the achievement of objectives.	There are processes for identifying and assessing risks and opportunities on a continuous basis. Risks are assessed to ensure consensus about the appropriate level of control, monitoring and reporting to carry out. Risk information is documented in a risk register.	Responses to the risks have been selected and implemented. There are processes for evaluating risks and responses implemented. The level of residual risk after applying mitigation techniques is accepted by the organisation, or further mitigations have been planned.	High quality, accurate and timely information is available to operational management and directors. The board reviews the risk management strategy, policy and approach on a regular basis, e.g. annually, and reviews key risks, emergent and new risks, and action plans on a regular basis, e.g. quarterly.	The organisational performance management framework and reward structure drives improvements in risk management. Risk management is a management competency. Management assurance is provided on the effectiveness of their risk management on a regular basis.
Managed	Risk management objectives are defined and management are trained in risk management techniques. Risk management is written into the performance expectations of managers. Management and executive level responsibilities for key risks have been allocated.	There are clear links between objectives and risks at all levels. Risk information is documented in a risk register. The organisation's risk appetite is used in the scoring system for assessing risks. All significant projects are routinely assessed for risk.	There is clarity over the risk level that is accepted within the organisation's risk appetite. Risk responses appropriate to satisfy the risk appetite of the organisation have been selected and implemented.	The board reviews key risks, emergent and new risks, and action plans on a regular basis, e.g. quarterly. It reviews the risk management strategy, policy and approach on a regular basis, e.g. annually. Directors require interim updates from delegated managers on individual risks which they have personal responsibility.	The organisation's risk management approach and the Board's risk appetite are regularly reviewed and refined in light of new risk information reported. Management assurance is provided on the effectiveness of their risk management on an ad hoc basis. The resources used in risk management become quantifiably cost effective. KPIs are set to improve certain aspects of the risk management activity, e.g. timeliness of implementation of risk responses, number of risks materialising or surpassing impact-likelihood expectations.
Defined	A risk strategy and policies are in place and communicated. The level of risk-taking that the organisation will accept is defined and understood in some parts of the organisation, and it is used to consider the most appropriate responses to the management of identified risks. Management and executive level responsibilities for key risks have been allocated.	There are processes for identifying and assessing risks and opportunities in some parts of the organisation but not consistently applied in all. All risks identified have been assessed with a defined scoring system. Risk information is brought together for some parts of the organisation. Most projects are assessed for risk.	Management in some parts of the organisation are familiar with, and able to distinguish between, the different options available in responding to risks to select the best response in the interest of the organisation.	Management have set up methods to monitor the proper operation of key processes, responses, and action plans. Management report risks to directors where responses have not managed the risks to a level acceptable to the board.	The Board gets minimal assurance on the effectiveness of risk management.
Aware	There is a scattered, silo-based approach to risk management. The vision, commitment and ownership of risk management have been documented. However, the organisation is reliant on a few key people for the knowledge, skills and the practice of risk management activities on a day-to-day basis.	A limited number of managers are trained in risk management techniques. There are processes for identifying and assessing risks and opportunities, but these are not fully comprehensive or implemented. There is no consistent scoring system for assessing risks. Risk information is not fully documented.	Some responses to the risks have been selected and implemented by management according to their own perception of risk appetite in the absence of a board-approved appetite for risk.	There are some monitoring processes and ad hoc reviews by some managers on risk management activities.	Management does not assure the Board on the effectiveness of risk management.
Naïve	No formal approach developed for risk management. No formal consideration of risks to business objectives, or clear ownership, accountability and responsibility for the management of key risks.	Processes for identifying and evaluating risks and responses are not defined. Risks have not been identified nor collated. There is no consistent scoring system for assessing risks.	Responses to the risks have not been designed or implemented.	There are no monitoring processes or regular reviews of risk management.	Management does not assure the Board on the effectiveness of risk management.

Aberdeen

45 Queen's Road
Aberdeen
AB15 4ZN

T: 01224 322100

Dundee

The Vision Building
20 Greenmarket
Dundee
DD1 4QB

T: 01382 200055

Edinburgh

Ground Floor
11-15 Thistle Street
Edinburgh
EH2 1DF

T: 0131 226 0200

Glasgow

100 West George Street
Glasgow
G2 1PP

T: 0141 471 9870

MHA Henderson Loggie is a trading name of Henderson Loggie LLP, which is a limited liability partnership registered in Scotland with registered number SO301630 and is a member of MHA, an independent member of Baker Tilly International Ltd, the members of which are separate and independent legal entities

© 2019 MHA Henderson Loggie



hlca.co.uk | info@hlca.co.uk