

SHETLAND UHI

# RISK MANAGEMENT

INTERNAL AUDIT REPORT - FINAL

APRIL 2023

## LEVEL OF ASSURANCE:

DESIGN	LIMITED
EFFECTIVENESS	LIMITED

IDEAS | PEOPLE | TRUST



# CONTENTS

1. <u>'EXECUTIVE SUMMARY'</u>	3
2. <u>DETAILED FINDINGS</u>	5
3. <u>BACKGROUND</u>	16
4. <u>RISK REGISTER TEMPLATE</u>	17
5. <u>BDO RISK MATURITY ASSESSMENT</u>	18
6. <u>DEFINITIONS</u>	19
7. <u>TERMS OF REFERENCE</u>	20
8. <u>STAFF INTERVIEWED</u>	21
9. <u>LIMITATIONS AND RESPONSIBILITIES</u>	22

## RESTRICTIONS OF USE

The matters raised in this report are only those which came to our attention during our audit and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made. The report has been prepared solely for the management of the organisation and should not be quoted in whole or in part without our prior written consent. BDO LLP neither owes nor accepts any duty to any third party whether in contract or in tort and shall not be liable, in respect of any loss, damage or expense which is caused by their reliance on this report.

DISTRIBUTION LIST		
FOR ACTION	JANE LEWIS	PRINCIPAL
	GEMMA MACGREGOR	DEPUTY PRINCIPAL (OPERATIONS)
FOR INFORMATION	AUDIT COMMITTEE	MEMBERS

REPORT STATUS	
LEAD AUDITOR(S):	GEMMA MACLEOD
DATES WORK PERFORMED:	20/02/2023 - 06/04/2023
DRAFT REPORT ISSUED:	17/04/2023
MANAGEMENT RESPONSES RECEIVED:	16/05/2023
FINAL REPORT ISSUED:	18/05/2023



# EXECUTIVE SUMMARY

LEVEL OF ASSURANCE: (SEE APPENDIX III FOR DEFINITIONS)		
DESIGN	Limited	System of internal controls is weakened with system objectives at risk of not being achieved.
EFFECTIVENESS	Limited	Non-compliance with key procedures and controls places the system objectives at risk.

SUMMARY OF FINDINGS (SEE APPENDIX III)			# OF AGREED ACTIONS
H	0		0
M	5		9
L	3		3
TOTAL NUMBER OF FINDINGS: 8			

## BACKGROUND

Risk management is fundamental to colleges to ensure potential threats are identified and analysed and steps are taken to prevent or minimise the impact of risks materialising.

The Scottish Public Finance Manual (SPFM) provides guidance on the basic principles of risk management. It expects that each public sector organisation’s internal control systems should include embedded arrangements for identifying, assessing, addressing, reviewing and reporting their risks. This should be integrated into normal management systems and closely linked to the business planning process. Each organisation’s governing body should make 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.

Detail on the key processes and practices in place in relation to risk management within SUHI are included in the Background section at appendix I.

## CONCLUSION

As part of our review, we have identified 8 findings, of which 5 were assessed as medium and 3 as low.

Shetland UHI (SUHI)’s control framework for risk management has been under development since the merger in 2021, but still lacks maturity.

SUHI has adopted the UHI Risk Management Policy and the UHI Common Risks for their use. There is no documentation which captures the risk management activities undertaken by SUHI separate to UHI. SUHI does not undertake any activity to identify risks specific to their own institution which may not be covered by the Common Risks and they do not have an operational risk register or a risk appetite statement in place.

SUHI provided risk management training to their Board of Management in October 2020 but have not yet provided training to any of their management or operational staff and there is no coverage of risk management in staff inductions.

As a result of our audit, we can provide limited assurance over the design and operational effectiveness of SUHI’s arrangements in place in relation to risk management. There may be gaps in SUHI’s risk coverage due to their reliance on the UHI Risk Management Policy and Common Risks only; whilst SUHI should continue to use these, they should be supplemented with risk management procedures and operational risk registers specific to SUHI.

In Appendix III we have included our Risk Maturity Assessment to further explain how we assess the risk management arrangements against good practice.



# EXECUTIVE SUMMARY

## PURPOSE

The purpose of this review is to provide assurance over the design and operational effectiveness of the key controls in risk management in the following areas:

- ▶ Suitable risk strategy and policy
- ▶ Identifying risks
- ▶ Assessing risks
- ▶ Addressing risks
- ▶ Reviewing, reporting and monitoring risks
- ▶ Risk management training

## SUMMARY OF GOOD PRACTICE

- ▶ The UHI Risk Management Policy which is used by SUHI is available to all staff on Sharepoint.
- ▶ At UHI level, there is a University Risk Review Group which performs regular horizon scanning.
- ▶ Risks are assessed based on likelihood and impact, which aligns with good practice.
- ▶ Risks are allocated to a Board Sub-committee for ownership.
- ▶ SUHIs Senior Management Group looks at a different risk in depth each fortnight.
- ▶ The Board completed risk management training in the form of a workshop in October 2020.

## SUMMARY OF HIGH AND MEDIUM FINDINGS


- ▶ We found that SUHI have adopted the UHI common risks and do not undertake risk identification activities of their own.
- ▶ SUHI does not have a formal risk appetite statement in place which defines their risk appetite for different categories of risk.
- ▶ SUHI follow the UHI Risk Management Policy but they do not have any documentation which outlines the processes or roles and responsibilities specific to SUHI.
- ▶ Whilst SUHI advised that the UHI Common Risks are provided in narrative form from UHI and then scored by the SUHI Senior Management Group, we were unable to find evidence in meeting minutes of the SMG challenging, reviewing or approving the scoring of risks on the risk register.
- ▶ SUHI have not provided risk management training to management or operational staff.

# DETAILED FINDINGS



# DETAILED FINDINGS


## RISK: THE COLLEGE MAY NOT HAVE SYSTEMATIC PROCESSES IN PLACE TO IDENTIFY RISKS

FINDING 1 - RISK IDENTIFICATION ACTIVITIES			TYPE
<p>It is important that SUHI has systematic processes in place to identify emerging risks.</p> <p>During testing we found that Shetland UHI have adopted the UHI Common Risks and has not identified their own risks. Risk identification exercises are completed at a Board and Senior Management Group Level, however do not undertake risk identification activities at an operational level</p>			DESIGN 
IMPLICATION			SIGNIFICANCE
There is a risk that SUHI may not identify risks specific to their organisation and these risks may therefore go unmanaged and may manifest.			MEDIUM
RECOMMENDATIONS	ACTION OWNER	MANAGEMENT RESPONSE	COMPLETION DATE
<p>Whilst we recommend that SUHI continue to use the UHI Common Risks as the basis for their Strategic Risk Register, we recommend that they undertake regular risk identification activities at an operational level.</p> <p>Examples of risk identification activities could include workshops, risk assessments, horizon scanning, or SWOT/PESTLE analyses.</p>	Professor Jane Lewis Principal & CEO Gemma MacGregor Vice Principal	<p>We partially accept the findings; our operational risks are embedded in the strategic risk(s) and therefore are reviewed regularly.</p> <p>We will however increase our risk identification activities such as the suggested examples and use to develop our operational actions based on our strategic risks.</p>	31 October 2023
<p>We recommend that in the risk management procedure referenced in recommendation three, SUHI records expected risk identification activities at a Board, SMT and operational level including frequency, documentation and the escalation process.</p>	Professor Jane Lewis Principal & CEO Gemma MacGregor Vice Principal Davie Sandison Chair of the Board	<p>We accept the findings in line with recommendation 3.</p>	31 October 2023



# DETAILED FINDINGS


**RISK: THE COLLEGE MAY NOT HAVE CLEARLY DOCUMENTED RISK MANAGEMENT PROCESSES AND PROCEDURES, INCLUDING ROLES AND RESPONSIBILITIES, ESCALATION PROTOCOLS AND REPORTING**

FINDING 2 - RISK APPETITE STATEMENT			TYPE
<p>It is important that the level of risk SUHI is willing to accept is agreed and understood across the organisation.</p> <p>We found that SUHI does not have a formal risk appetite statement in place which defines their risk appetite for different categories of risk.</p>			DESIGN 
IMPLICATION			SIGNIFICANCE
<p>There is a risk that it is currently unclear what a tolerable level of risk is to SUHI and therefore SUHI may not mitigate risks to an appropriate level or may be exposed to an unacceptable level of risk.</p>			MEDIUM
RECOMMENDATIONS	ACTION OWNER	MANAGEMENT RESPONSE	COMPLETION DATE
<p>We recommend that SUHI develops a Risk Appetite Statement which defines their risk appetite (e.g. averse, minimal, cautious, open) for different categories of risk (e.g. governance and compliance, reputational, financial, people). Each risk on the register should be assigned to a risk category and the target risk level should align to the risk appetite. The Risk Appetite should be regularly reviewed by the Board or relevant sub-committee. Guidance on developing a risk appetite statement can be found at <a href="#">Risk Appetite Guidance Note (publishing.service.gov.uk)</a></p>	Davie Sandison Chair of the Board Professor Jane Lewis Principal and CEO	We accept the findings and recommendations.	31 October 2023



# DETAILED FINDINGS

**RISK: THE COLLEGE MAY NOT HAVE CLEARLY DOCUMENTED RISK MANAGEMENT PROCESSES AND PROCEDURES, INCLUDING ROLES AND RESPONSIBILITIES, ESCALATION PROTOCOLS AND REPORTING**


FINDING 3 - DOCUMENTATION OF SUHI RISK MANAGEMENT PROCEDURES			TYPE
<p>It is important that SUHI has clearly documented guidance in place which outlines their expected risk management procedures.</p> <p>We found that SUHI follow the UHI Risk Management Policy but that they do not have any documentation which outlines the processes or roles and responsibilities specific to Shetland UHI.</p>			DESIGN 
IMPLICATION			SIGNIFICANCE
There is a risk that there may not be clear guidance for staff on the full risk management process in order to help them understand their roles and responsibilities.			MEDIUM
RECOMMENDATIONS	ACTION OWNER	MANAGEMENT RESPONSE	COMPLETION DATE
<p>We recommend that SUHI develop their own risk management procedures specific to their risk management arrangements and protocols to support the existing UHI Risk Management Policy. The Procedures should contain the following:</p> <ul style="list-style-type: none"> <li>• Risk appetite arrangements;</li> <li>• Roles and responsibilities of all individuals and committees involved in risk management;</li> <li>• Detail of Shetland UHI’s risk management processes including; risk identification and assessment, risk treatment, risk monitoring and risk reporting;</li> <li>• Details of the types of risk register in operation, and the processes for escalating and de-escalating risks;</li> <li>• Review arrangements for the Procedures.</li> </ul>	Gemma MacGregor Vice Principal	We accept the findings and will undertake the development of the recommendations of a risk management procedure to support the existing uhi risk management policy.	31 October 2023





# DETAILED FINDINGS


## RISK: THE COLLEGE MAY NOT HAVE SYSTEMATIC PROCESSES IN PLACE TO ASSESS RISKS

FINDING 4 - RISK ASSESSMENT PROCESSES			TYPE
<p>It is important that there are established processes in place to consistently and effectively score risks.</p> <p>SUHI advised that the UHI Common Risks are provided in narrative form from UHI and are then scored by the Shetland UHI Senior Management Group. However, we were unable to find evidence in meeting minutes of the SMG challenging, reviewing or approving the scoring of risks on the risk register.</p>			<b>EFFECTIVENESS</b> 
IMPLICATION			SIGNIFICANCE
<p>There is a risk that, without a robust risk assessment and scoring approach, the scoring of risks may not accurately represent the potential impact of risks on <b>SUHI</b> and the likelihood of their occurrence.</p>			<b>MEDIUM</b>
RECOMMENDATIONS	ACTION OWNER	MANAGEMENT RESPONSE	COMPLETION DATE
We recommend that the process for assessing and scoring risks is captured in the Risk Management Procedures including when this should be done and who is responsible.	Gemma MacGregor Vice Principal	We accept the findings and the recommendations in line with finding 3.	31 October 2023
We recommend that changes to risks and risk scorings by the SMG are recorded.	Gemma MacGregor Vice Principal	We accept the findings and recommendations in conjunction with the development of the recommendations in finding 2.	31 October 2023



# DETAILED FINDINGS


## RISK: THE COLLEGE MAY NOT BE PROVIDING APPROPRIATE RISK MANAGEMENT TRAINING TO RELEVANT STAFF

FINDING 5 - RISK MANAGEMENT TRAINING			TYPE
<p>It is important that staff receive suitable training in the risk management procedures.</p> <p>Shetland UHI have not yet provided risk management training to management or operational staff. We also found that Risk Management is not included in staff inductions. Although risk management training was provided to the Board in October 2020, there is currently no planned training for new Board members or refresher training for continuing members.</p>			<p>DESIGN &amp; EFFECTIVENESS</p> 
IMPLICATION			SIGNIFICANCE
There is a risk that staff may not be fully equipped to execute their role and responsibilities related to risk management.			MEDIUM
RECOMMENDATIONS	ACTION OWNER	MANAGEMENT RESPONSE	COMPLETION DATE
We recommend that all staff receive regular training in risk management, suitable for their role. Risk Management should form part of the staff induction; as a minimum new staff should be required to read the Risk Management Policy.	<p>Professor Jane Lewis Principal and CEO</p> <p>Gemma MacGregor Vice Principal</p>	We accept the findings and this recommendation for staff training suitable for roles.	31 October 2023
We recommend that the Board receive refresher risk management training on a regular basis for example every three years.	Davie Sandison Chair of the Board	We accept the findings and this recommendation for refresher risk management training.	31 July 2025
We recommend that risk management training requirements are captured in the Risk Management Procedures	Gemma MacGregor Vice Principal	In line with finding and recommendation 3 we accept the recommendation.	31 October 2023



# DETAILED FINDINGS


## RISK: THE COLLEGE MAY NOT HAVE CLEARLY SET OUT ITS STRATEGIC DIRECTION AND OBJECTIVES IN RELATION TO RISK MANAGEMENT

FINDING 6 - RISK MANAGEMENT OBJECTIVES			TYPE
<p>It is important that SUHI has clear strategic direction and achievable objectives in relation to risk management.</p> <p>The UHI Risk Management Policy which is used by Shetland UHI does not include risk management objectives. We were therefore unable to confirm that Shetland UHI's risk management objectives align with their Strategic Objectives.</p>			DESIGN 
IMPLICATION			SIGNIFICANCE
<p>There is a risk that SUHI is not working towards clear goals that contribute to their overall strategic direction.</p>			LOW
RECOMMENDATIONS	ACTION OWNER	MANAGEMENT RESPONSE	COMPLETION DATE
<p>We recommend that SUHI identifies a set of risk management objectives which align to their Strategic Objectives and that these are recorded within the Risk Management Procedures.</p>	<p>Gemma MacGregor Vice Principal</p>	<p>We will take it under advisement and consult with the board of management audit committee</p>	<p>End of June 2023</p>



# DETAILED FINDINGS

## RISK: THE COLLEGE MAY NOT HAVE SYSTEMATIC PROCESSES IN PLACE FOR ADDRESSING RISKS

FINDING 7 - RISK REGISTER			TYPE
<p>It is important that all risks are captured in a useful way on the risk register to allow them to be properly addressed.</p> <p>We identified the following areas where improvement could be made to the Shetland UHI risk register:</p> <ul style="list-style-type: none"> <li>• Shetland UHI do not attribute a target risk score to risks.</li> <li>• There is no assessment of the effectiveness of controls in place.</li> <li>• Risks are not linked to strategic objectives.</li> <li>• The risk register does not record which type of approach from the UHI Risk Management Policy is being taken i.e. tolerate, treat, transfer, terminate.</li> <li>• The action owner was not consistently recorded for risks in the extract we were provided and expected completion dates were not populated for any of the actions.</li> <li>• The risk category was not consistently recorded for risks in the extract we were provided.</li> </ul>			DESIGN 
IMPLICATION			SIGNIFICANCE
<p>There is a risk that the current risk register format does not provide all necessary information to provide users with a full understanding of the risk and how it is being managed.</p>			LOW
RECOMMENDATIONS	ACTION OWNER	MANAGEMENT RESPONSE	COMPLETION DATE
<i>(overleaf)</i>			



# DETAILED FINDINGS


## RISK: THE COLLEGE MAY NOT HAVE SYSTEMATIC PROCESSES IN PLACE FOR ADDRESSING RISKS

FINDING 7 - RISK REGISTER			TYPE
RECOMMENDATIONS	ACTION OWNER	MANAGEMENT RESPONSE	COMPLETION DATE
<p>We recommend that SUHI takes the following steps to improve their risk register format:</p> <ul style="list-style-type: none"> <li>• Each risk should be given a target risk score which aligns to the risk appetite for that category of risk to show what an acceptable level of risk is and where further mitigation is required.</li> <li>• For each risk, an assessment should be made of the effectiveness of controls in place e.g. effective, partly effective, ineffective.</li> <li>• Risks should be linked to Strategic Objectives to allow SUHI to effectively prioritise risks and allocate resources.</li> <li>• The risk approach (tolerate, treat, transfer, terminate) should be recorded for each risk.</li> <li>• Action owners and expected action completion dates should be consistently populated for all risks.</li> <li>• The risk category should be populated for each risk.</li> </ul> <p>An example risk register layout has been included at appendix II.</p>	<p>Professor Jane Lewis Principal and CEO</p> <p>Gemma MacGregor Vice Principal</p>	<p>We accept the findings and the recommendations that are noted and exemplified in the appendix ii layout.</p>	<p>01 March 2024</p>



# DETAILED FINDINGS

## RISK: THE COLLEGE MAY NOT HAVE ADEQUATE REPORTING IN PLACE TO MANAGEMENT AND THE BOARD AND ITS RELEVANT SUB-COMMITTEES IN RELATION TO RISK MANAGEMENT ACTIVITIES

FINDING 8 - REPORTING TO BOARD OF MANAGEMENT			TYPE
<p>It is important that management and the Board of Management have sufficient oversight of risk management performance.</p> <p>The expected risk review process within SUHI is not documented.</p> <p>Whilst we found that there was suitable reporting to the Senior Management Group, risk reporting to the Board of Management or relevant sub-committee has not taken place with suitable regularity to date. Risk management was not reported to the Board of Management at any of their 2021/22 meetings; SUHI noted that initially Board meetings were more operational in their focus following the merger. When the Board did review the riskregister at their meeting on 24/08/22, there was no evidence of challenge of risk management in the meeting minutes. Furthermore the Audit Committee has not been meeting regularly do to issues with meeting quorum.</p>			<b>DESIGN &amp; EFFECTIVENESS</b> 
IMPLICATION			
There is a risk that the Board of Management have not had enough oversight of risk management performance to date to provide effective challenge.			LOW
RECOMMENDATIONS	ACTION OWNER	MANAGEMENT RESPONSE	COMPLETION DATE
We recommend that, going forward, the Audit Committee review the Strategic Risk Register at each of their quarterly meetings and that they are encouraged to challenge the management of risks where appropriate. The Risk Register should also be circulated to the Board of Management.	Davie Sandison Chair of the Board	We accept the findings and will accept the recommendations.	01 March 2023

# APPENDICES



# APPENDIX I: BACKGROUND

## BACKGROUND

Shetland UHI (SUHI) took the decision on establishment, not to create policies where one already existed that they could use, therefore they have adopted the UHI Risk Management Policy. The Policy includes a risk policy statement which states that the general approach is to minimise the organisation's exposure to risk but in pursuit of the University's mission and objectives, it may choose to accept an increased level of risk.

The UHI Risk Management Policy was last reviewed in October 2022 and is next due for review in 2024. The Policy is stored on the SUHI Sharepoint and is accessible to all staff.

The Principal has overarching responsibility for supporting the risk identification, management and governance arrangements at SUHI.

SUHI have a Strategic Risk Register which is made up of the 13 UHI Common Risks and they are required to report to UHI under these risks.

At a UHI level, there is a University Risk Review Group which meets quarterly and routinely scans the horizon for new risks. Any new risks are shared with Academic Partners via email and at the Partnership Council. SUHI will then take these to their Senior Management Group (SMG) to discuss what underpins the risk and how they will mitigate it. The risk description is common across each Academic Partner's risk register but scoring and mitigation depends on local circumstances.

SUHI use the likelihood and impact scoring criteria outlined in UHI's Risk Management Policy for scoring risks. Each risk has a gross and residual risk score and there is a heat map included within the risk register which shows whether a risk is green, amber or red based on its score.

Per the UHI Risk Management Policy, there are four approaches available to managing risks as follows:

- Terminate - avoid the risk by doing something else;
- Transfer - the risk is passed on to someone else e.g. outsourcing, insurance, subcontracting;
- Treat - reduce the risk by management action; and
- Tolerate - accept the risk and manage it appropriately.

The SUHI Risk Register includes the following details for each of the risks:

- Risk reference
- Risk status
- Risk category
- Risk description
- Causes
- Owner
- Likelihood
- Impact
- Gross risk score
- Mitigating actions
- Residual likelihood
- Residual impact
- Residual risk score
- Action plan (actions with owners and completion dates)

The SUHI SMG conducts a deep dive into a different risk each fortnight with risks chosen based on either current events or the age of the risk. Each Board Sub-Committee meets on a quarterly basis and is empowered to decide how frequently they review any risks under their ownership.

SUHI provided their Board of Management with a risk management training workshop in October 2020. Training covered basic definitions of risk, risk assessment and recording, monitoring and challenging risks, common risks, and dynamic reporting.





# APPENDIX II: RISK REGISTER TEMPLATE

Risk Ref.	Risk	Strategic Objective	Risk Category	Inherent Risk			Controls	Type	Control Effectiveness	Residual Risk			Risk Appetite	Target Risk			Actions	Action Owner / Deadline
				Probability	Impact	Score				Probability	Impact	Score		Probability	Impact	Score		
1	College does not achieve allocated HE student number targets	Strategic Objective X	Strategy	5	4	20	Control 1	Preventative	Effective / Partial / Not Effective	3	4	12	Cautious	3	2	6	Action 1	Owner / Deadline
							Control 2	Detective									Effective / Partial / Not Effective	Action 2



# APPENDIX III: BDO RISK MATURITY ASSESSMENT

	Risk Governance	Risk Identification and Assessment	Risk Mitigation and Treatment	Risk Reporting and Review	Continuous Improvement
<b>Enabled</b>	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.
<b>Managed</b>	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.
<b>Defined</b>	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.
<b>Aware</b>	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.
<b>Naïve</b>	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.



# APPENDIX IV: DEFINITIONS

LEVEL OF ASSURANCE	DESIGN OF INTERNAL CONTROL FRAMEWORK		OPERATIONAL EFFECTIVENESS OF CONTROLS	
	FINDINGS FROM REVIEW	DESIGN OPINION	FINDINGS FROM REVIEW	EFFECTIVENESS OPINION
<b>SUBSTANTIAL</b>	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.
<b>MODERATE</b>	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.
<b>LIMITED</b>	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.
<b>NO</b>	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	
<b>HIGH</b>	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.
<b>MEDIUM</b>	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.
<b>LOW</b>	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.
<b>ADVISORY</b>	A weakness that does not have a risk impact or consequence but has been raised to highlight areas of inefficiencies or potential best practice improvements.



# APPENDIX V: TERMS OF REFERENCE

## EXTRACT FROM TERMS OF REFERENCE

### PURPOSE

The purpose of this review is to provide assurance over the design and operational effectiveness of the key controls in risk management in the following areas:

- Suitable risk strategy and policy
- Identifying risks
- Assessing risks
- Addressing risks
- Reviewing, reporting and monitoring risks
- Risk management training

### KEY RISKS

1. The college may not have clearly set out its strategic direction and objectives in relation to risk management.
2. The college may not have clearly documented risk management processes and procedures, including roles and responsibilities, escalation protocols and reporting.
3. The college may not have systematic processes in place to identify risks.
4. The college may not have systematic processes in place to assess risks.
5. The college may not have systematic processes in place for addressing risks.
6. The college may not have adequate reporting in place to management and the Board and its relevant sub-committees in relation to risk management activities.
7. The college may not be providing appropriate risk management training to relevant staff.

### EXCLUSIONS/LIMITATIONS OF SCOPE

The scope of the review is limited to the areas documented under the scope and approach. All other areas are considered outside of the scope of this review.

Our work is inherently limited by sampling operational risk registers and monitoring arrangements and therefore will not provide assurance over all risk management processes within the college. We are reliant on the honest representation by staff and timely provision of information as part of this review.



## APPENDIX VI: 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.

JANE LEWIS	PRINCIPAL	AUDIT SPONSOR
GEMMA MACGREGOR	VICE PRINCIPAL (OPERATIONS)	AUDIT LEAD



## APPENDIX VII: LIMITATIONS AND RESPONSIBILITIES

### MANAGEMENT RESPONSIBILITIES

The Audit Committee is responsible for determining the scope of internal audit work, and for deciding the action to be taken on the outcome of our findings from our work. The Committee is also responsible for ensuring the internal audit function has:

- The support of the management team.
- Direct access and freedom to report to senior management, including the Chair of the Audit Committee.

The Board is responsible for the establishment and proper operation of a system of internal control, including proper accounting records and other management information suitable for running the College.

Internal controls covers the whole system of controls, financial and otherwise, established by the Board in order to carry on the business of the College in an orderly and efficient manner, ensure adherence to management policies, safeguard the assets and secure as far as possible the completeness and accuracy of the records. The individual components of an internal control system are known as 'controls' or 'internal controls'.

The Board is responsible for risk management in the organisation, and for deciding the action to be taken on the outcome of any findings from our work. The identification of risks and the strategies put in place to deal with identified risks remain the sole responsibility of the Board.

### LIMITATIONS

The scope of the review is limited to the areas documented under Appendix II - Terms of reference. All other areas are considered outside of the scope of this review.

Our work is inherently limited by the honest representation of those interviewed as part of colleagues interviewed as part of the review. Our work and conclusion is subject to sampling risk, which means that our work may not be representative of the full population.

Internal control systems, no matter how well designed and operated, are affected by inherent limitations. These include the possibility of poor judgment in decision-making, human error, control processes being deliberately circumvented by employees and others, management overriding controls and the occurrence of unforeseeable circumstances.

Our assessment of controls is for the period specified only. Historic evaluation of effectiveness may not be relevant to future periods due to the risk that: the design of controls may become inadequate because of changes in operating environment, law, regulation or other; or the degree of compliance with policies and procedures may deteriorate.

## FOR MORE INFORMATION:

**CLAIRE ROBERTSON, DIRECTOR**

+44 (0)141 249 5206

Claire.robertson@bdo.co.uk

### Freedom of Information

In the event you are required to disclose any information contained in this report by virtue of the Freedom of Information Act 2000 (“the Act”), you must notify BDO LLP promptly prior to any disclosure. You agree to pay due regard to any representations which BDO LLP makes in connection with such disclosure, and you shall apply any relevant exemptions which may exist under the Act. If, following consultation with BDO LLP, you disclose this report in whole or in part, you shall ensure that any disclaimer which BDO LLP has included, or may subsequently wish to include, is reproduced in full in any copies.

### Disclaimer

This publication has been carefully prepared, but it has been written in general terms and should be seen as containing broad statements only. This publication should not be used or relied upon to cover specific situations and you should not act, or refrain from acting, upon the information contained in this publication without obtaining specific professional advice. Please contact BDO LLP to discuss these matters in the context of your particular circumstances. BDO LLP, its partners, employees and agents do not accept or assume any responsibility or duty of care in respect of any use of or reliance on this publication, and will deny any liability for any loss arising from any action taken or not taken or decision made by anyone in reliance on this publication or any part of it. Any use of this publication or reliance on it for any purpose or in any context is therefore at your own risk, without any right of recourse against BDO LLP or any of its partners, employees or agents.

BDO LLP, a UK limited liability partnership registered in England and Wales under number OC305127, is a member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. A list of members' names is open to inspection at our registered office, 55 Baker Street, London W1U 7EU. BDO LLP is authorised and regulated by the Financial Conduct Authority to conduct investment business.

BDO is the brand name of the BDO network and for each of the BDO member firms.

BDO Northern Ireland, a partnership formed in and under the laws of Northern Ireland, is licensed to operate within the international BDO network of independent member firms.

The matters raised in this report are only those which came to our attention during our audit and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made. The report has been prepared solely for the management of the organisation and should not be quoted in whole or in part without our prior written consent. BDO LLP neither owes nor accepts any duty to any third party whether in contract or in tort and shall not be liable, in respect of any loss, damage or expense which is caused by their reliance on this report.

Copyright ©2023 BDO LLP. All rights reserved. Published in the UK.

[www.bdo.co.uk](http://www.bdo.co.uk)