

SHETLAND UHI

BUSINESS CONTINUITY PLANNING

INTERNAL AUDIT REPORT - FINAL

JUNE 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>OBSERVATIONS</u>	14
4. <u>BACKGROUND</u>	16
5. <u>DEFINITIONS</u>	17
6. <u>TERMS OF REFERENCE</u>	18
7. <u>STAFF INTERVIEWED</u>	19
8. <u>LIMITATIONS AND RESPONSIBILITIES</u>	20

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	GEMMA MACGREGOR	VICE PRINCIPAL (OPERATIONS)
FOR INFORMATION	AUDIT COMMITTEE	MEMBERS

REPORT STATUS	
LEAD AUDITOR(S):	GEMMA MACLEOD
DATES WORK PERFORMED:	17 APRIL - 30 MAY 2023
ADDITIONAL DOCUMENTATION RECEIVED:	12 JUNE 2023
DRAFT REPORT ISSUED:	21 JUNE 2023
MANAGEMENT RESPONSES RECEIVED:	20 JULY 2023
FINAL REPORT ISSUED:	27 JULY 2023



EXECUTIVE SUMMARY

LEVEL OF ASSURANCE: (SEE APPENDIX II 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	1		2
M	4		6
L	3		3
TOTAL NUMBER OF FINDINGS: 8			

BACKGROUND

Business continuity planning is key to the sustainability of an organisation’s operations should an adverse event or situation arise. Business continuity should be a holistic management process that identifies potential events that could cause disruption to business operations and the plans that enable the organisation to continue to perform its key activities outside of normal operating conditions or in the midst of disruptive events.

Covid-19 has meant that most organisations are now set up to work remotely, however there are potential situations the UHI Shetland (the College) should be prepared for, for example power cuts.

In accordance with the 2022-23 Internal Audit Plan, it was agreed that internal audit would review the business continuity planning arrangements within the College.

Details of key business continuity arrangements in place within the College can be found at Appendix I.

PURPOSE

The purpose of the review is to provide assurance over the design and operational effectiveness of the college’s business continuity planning arrangements in the following areas:

- Roles and responsibilities
- Critical systems
- Suitability
- Testing
- Communication
- Location
- Contact Details.

CONCLUSION

As part of our review, we have identified 9 findings, of which 1 was assessed as high, 4 were assessed as medium and 3 as low.

We found that the system of internal control surrounding business continuity planned is weakened, and we can provide a limited level of assurance over the design and operational effectiveness of the arrangements in place.

SUMMARY OF HIGH AND MEDIUM FINDINGS


- ▶ SUHI has not completed a risk assessment to identify all business critical systems and functions. There is no consideration of the minimum level of resources required to deliver the functions and impact assessments have not been completed to identify the maximum time that a function could remain undelivered, or what the impact would be if the function remained undelivered for longer. Due to this, action plans for restoration are not in place for each function and system.
- ▶ The BCP does not detail incidents that could cause it to be utilised, along with the specific procedures to be followed for each, and applicable timescales.
- ▶ The BCP does not give consideration of individual staff roles and responsibilities that are relevant to business continuity.
- ▶ There has been no previous testing of the BCP, and there are currently no formal plans in place for testing to take place on a regular basis.
- ▶ There has been no training provided to staff in relation to business continuity.

DETAILED FINDINGS



DETAILED FINDINGS


RISK: THE COLLEGE MAY NOT HAVE DEFINED ITS BUSINESS-CRITICAL SYSTEMS AND PROCESSES.

FINDING 1 - BUSINESS CRITICAL SYSTEMS AND FUNCTIONS			TYPE
<p>It is important to understand the business critical functions and systems, and plan for the recovery of these within target timescales during an incident.</p> <p>The Business Continuity Plan lists some business critical functions, however these are limited.</p> <p>SUHI has not performed a risk assessment to identify business critical systems and functions. In addition, there is no consideration of the minimum level of resources required to deliver the functions and it does not include impact assessments to identify the maximum time that a function could remain undelivered, or what the impact would be if the function remained undelivered for longer.</p> <p>Due to this, action plans for restoration are not in place for each function and system. We do recognise that a recovery action plan and activity list are documented within the BCP, however these do not provide a detailed account of recovery for each function and system.</p>			<p>DESIGN & EFFECTIVENESS</p> 
IMPLICATION			SIGNIFICANCE
<p>There is a risk that SUHI's critical functions and systems cannot be effectively restored following a disruption due to a lack of planning and analysis of these. There is also the risk that the impact of downtime has not been fully assessed and that the timescales required for recovery have not been fully analysed.</p>			HIGH
RECOMMENDATIONS	ACTION OWNER	MANAGEMENT RESPONSE	COMPLETION DATE
<p>We recommend that SUHI performs a risk assessment to identify all business critical functions and systems, and the minimum resources required to operate these. In addition, an impact assessment should be undertaken for each, and should be used to set a maximum allowable time to recover operations, and a target recovery time.</p>	Gemma MacGregor/Angela Sutherland / Michael Nisbet	Partial acceptance; we can identify all business critical functions and systems but in the case of the ICT systems we are unable to set recovery targets (and by extension impact assessments locally) as they are controlled by uhi executive office.	31 July 2023
<p>Upon completion of the above, we recommend that clear action plans are developed for each business critical system or function. The action plan should document the process to be followed in the event of disruption, actions to be taken and procedures to be followed for restoration, and should be designed to achieve intended recovery times. It would be beneficial to record the above in a checklist-type, easy to read format.</p>	Gemma MacGregor/Angela Sutherland / Michael Nisbet	As above; not applicable for vast majority of ict functions as it is outwith our control	31 July 2023



DETAILED FINDINGS


RISK: THE PLAN MAY NOT BE SUITABLE TO ALLOW THE COLLEGE TO RECOVER FROM A SIGNIFICANT DISRUPTION WITHIN THE REQUIRED TIMESCALES.

FINDING 2 - EXAMPLE INCIDENTS AND ACTION PLANS			TYPE
<p>Effective BCPs require clear action plans for business continuity events in order for organisations to recover efficiently from such events. The BCP does not detail incidents that could cause it to be utilised, along with the specific procedures to be followed for each and applicable timescales.</p>			<p>DESIGN </p>
<p>IMPLICATION</p> <p>There is a risk that SUHI has not considered all potential incidents, and how it would react to these.</p>			<p>SIGNIFICANCE</p> <p>MEDIUM</p>
RECOMMENDATIONS	ACTION OWNER	MANAGEMENT RESPONSE	COMPLETION DATE
<p>We recommend that SUHI documents a range of incidents that could cause the BCP to be enforced, along with the procedures to be followed for each in a 'check list' format. Example incidents could include fire evacuation, a serious medical emergency, severe weather, terrorist threat, power failure and loss of gas supply. The above should be recorded in a checklist-type, easy to read format.</p>	<p>Gemma MacGregor/ Angela Sutherland</p>	<p>Accept however this list can never be exhaustive and we feel it is more important to remain agile and able to react to situations as they arrive. *mains Gas supply not available in islands*</p>	<p>01 September 2023</p>



DETAILED FINDINGS


RISK: ROLES AND RESPONSIBILITIES MAY NOT BE DEFINED IN THE BUSINESS CONTINUITY PLAN (BCP).

FINDING 3 - ROLES AND RESPONSIBILITIES			TYPE
<p>It is important that key teams or roles are identified in managing and responding to a business disruptive incident.</p> <p>The BCP does not give consideration of individual staff roles and responsibilities that are relevant to business continuity. In addition, members of the core BTC Team are listed, but the role and responsibilities of this team have not been documented.</p> <p>Also, the BCP does not provide details of who assumes key roles in a disaster or crisis, including fire marshals and first aiders.</p>			DESIGN 
IMPLICATION			SIGNIFICANCE
There is a risk that any incident may not be responded to appropriately due a lack of documented responsibilities.			MEDIUM
RECOMMENDATIONS	ACTION OWNER	MANAGEMENT RESPONSE	COMPLETION DATE
We recommend that the BCP is updated to provide a detailed account of responsibilities for each relevant staff member. In addition, key roles and their responsibilities should also be confirmed, including first aiders and fire marshals. We also recommend that the responsibilities of the core BCT Team should be clearly documented within the BCP.	Gemma MacGregor / Angela Sutherland	Accept	01 September 2023
Lastly, it should be ensured that required updates to roles and responsibilities are monitored and made immediately, particularly following any staffing changes to ensure these remain accurate.	Gemma MacGregor / Kathy MacDonald	Accept	30 September 2023



DETAILED FINDINGS


RISK: THE BCP MAY NOT BE REGULARLY TESTED AND RESULTS REPORTED TO MANAGEMENT.

FINDING 4 - TESTING			TYPE
<p>In order to gain assurance that recovery strategies, and the BCP in general are effective in the event of a business disruption, it is important that plans are tested on a regular basis.</p> <p>There has been no previous testing of the BCP, and there are currently no formal plans in place for testing to take place on a regular basis.</p>			DESIGN 
IMPLICATION			SIGNIFICANCE
<p>There is a risk that the BCP may not be effective, and that this will only become apparent when a disruption to a business critical process occurs.</p>			MEDIUM
RECOMMENDATIONS	ACTION OWNER	MANAGEMENT RESPONSE	COMPLETION DATE
<p>We recommend that SUHI develops a testing plan/schedule for business continuity which should be reviewed regularly to ensure a strategic approach to testing is developed and implemented. This plan should ensure that varying categories of events are scheduled to be tested on a regular basis, based upon the likelihood and overall risk.</p>	Gemma MacGregor/ Angela Sutherland	Accept; a schedule will be developed	30 September 2023
<p>We recommend that outcomes (including confirmation of the achievement of recovery times), lessons learned and required actions are formally documented, and thereafter reflected within the plan for each test.</p>	Gemma MacGregor/ Angela Sutherland	Accept in line with above recommendation	30 September 2023



DETAILED FINDINGS


RISK: THE BCP MAY NOT BE APPROPRIATELY COMMUNICATED TO STAFF AND KEY STAFF MAY NOT BE AWARE OF THEIR ROLES IN THE PLAN.

FINDING 5 - TRAINING			TYPE
<p>Training is essential in ensuring that staff are aware of the required actions to be taken in responding to a business disruptive event.</p> <p>There has been no training provided to all staff in relation to business continuity.</p>			DESIGN 
IMPLICATION			SIGNIFICANCE
<p>There is a risk that staff are not aware of current business continuity procedures or their roles in instigating the plan.</p>			MEDIUM
RECOMMENDATIONS	ACTION OWNER	MANAGEMENT RESPONSE	COMPLETION DATE
<p>We recommend that the College implements business continuity training for relevant staff. Regular refresher training should be provided going forward (for example, every three years), and the College should ensure it maintains sufficient evidence of attendance/completion.</p>	<p>Gemma MacGregor / Angela Sutherland</p>	<p>Accept: Internal training will be planned for autumn 2023</p>	<p>31 October 2023</p>



DETAILED FINDINGS


RISK: THE PLAN MAY NOT BE SUITABLE TO ALLOW THE COLLEGE TO RECOVER FROM A SIGNIFICANT DISRUPTION WITHIN THE REQUIRED TIMESCALES.

FINDING 6 - APPROVAL OF BCP			TYPE
<p>It is expected that the BCP is reviewed and approved on a regular basis, to ensure the plans remain suitable to allow the Colege to recover from a disruptive incident.</p> <p>Version control within the BCP states that it was most recently reviewed and updated in March 2023, and indicates that it is reviewed on an annual basis. Internal Audit were advised that minutes of the Operations and Estates Committee meeting in April 2023 would evidence the approval of the BCP, however the minutes do not support this.</p>			DESIGN 
IMPLICATION			SIGNIFICANCE
There is a risk that the information within the BCP and supporting documentation is insufficient and not subject to appropriate approval and oversight.			LOW
RECOMMENDATIONS	ACTION OWNER	MANAGEMENT RESPONSE	COMPLETION DATE
We recommend that the BCP is submitted for approval, and that meeting minutes clearly evidence the approval.	Gemma MacGregor	Accept however this has been minuted at operations and estates committee previously	30 August 2023



DETAILED FINDINGS

RISK: THE BCP MAY NOT BE IN A SUITABLE LOCATION TO ALLOW IT TO BE PUT INTO EFFECT IN THE EVENT OF AN EMERGENCY SITUATION.

FINDING 7 - ACCESS TO THE BCP			TYPE
<p>It is important that key contacts have access to the BCP, should an event or incident occur that requires the Plans to be enacted.</p> <p>Internal Audit were provided with screenshots showing who had access to the full BCP onsharepoint and found that two people who have access are not included as key persons within the BCP itself. In addition, a key person listed within the BCP does not havesharepoint membership.</p>			EFFECTIVENESS 
IMPLICATION			SIGNIFICANCE
<p>There is a risk that key staff do not have appropriate access to the current BCP, which may result in the BCP not being effectively instigated when required. There is also a risk that access to the BCP is not appropriately restricted.</p>			LOW
RECOMMENDATIONS	ACTION OWNER	MANAGEMENT RESPONSE	COMPLETION DATE
<p>We recommend that the College ensures that those given access to the full version of the BCP aligns to the key persons documented within the BCP, to ensure access is appropriately controlled.</p>	Gemma Macgregor	Accept: BCP sharepoint updated and will be accessible by those in BCP	30 September 2023



DETAILED FINDINGS

RISK: THE PLAN MAY NOT BE SUITABLE TO ALLOW THE COLLEGE TO RECOVER FROM A SIGNIFICANT DISRUPTION WITHIN THE REQUIRED TIMESCALES.

FINDING 8 - BUSINESS CONTINUITY RISKS			TYPE
It is important that risks surrounding business continuity are identified and recorded to ensure that the risks can be appropriately managed. Management have not identified and formally documented business continuity risks within the SUHI risk register.			DESIGN
IMPLICATION			SIGNIFICANCE
There is a risk that business continuity risks and the impact of these are not identified and effectively managed, which could be detrimental to SUHI.			LOW
RECOMMENDATIONS	ACTION OWNER	MANAGEMENT RESPONSE	COMPLETION DATE
We recommend that management collectively consider any business continuity risks, and that these are documented and managed in line with SUHUI's risk management processes.		Reject: we use the UHI Framework for risk management and would not propose adding a BCP risk.	

OBSERVATIONS



OBSERVATIONS

IT DISASTER RECOVERY PLAN

We found the College does not have a fully documented IT Disaster Recovery Plan that details the recovery steps for IT incidents that would affect the College directly. We understand that the ICT function and all associated disaster recovery plans are the responsibility of the UHI Executive Office and therefore the College does not have the authority to create an IT Disaster Recovery Plan which includes Recovery Time Objectives and Maximum Tolerable Periods of Disruption

APPENDICES



APPENDIX I: BACKGROUND

SUHI has developed a Business Continuity Plan (BCP), with the purpose being to set out procedures for activating in the case of a major loss of disruption of business. The BCP applies to all staff and students of SUHI.

The Principal, Depute Principal, Vice Principal and Head of Finance all have the power to invoke the BCP. The BCP itself details the core BCP team, which includes the Principal, Business and Projects Officer, Vice Principal and Depute Principal amongst others, along with other key staff such as the Head of Facilities and Finance Officer.

Functions critical to the business are listed as ICT, Payroll, Health & Safety and Estates/Buildings.

Critical contacts are listed along with their details, including Shetland Island's Council, Zurich and NFU Mutual.



APPENDIX II: DEFINITIONS

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

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

EXTRACT FROM TERMS OF REFERENCE

PURPOSE

The purpose of the review is to provide assurance over the design and operational effectiveness of the college's business continuity planning arrangements in the following areas:

- Roles and responsibilities
- Critical systems
- Suitability
- Testing
- Communication
- Location
- Contact Details

KEY RISKS

1. Roles and responsibilities may not be defined in the Business Continuity Plan (BCP).
2. The College may not have defined its business critical systems and processes.
3. The plan may not be suitable to allow the college to recover from a significant disruption within the required timescales.
4. The BCP may not be regularly tested and results reported to management.
5. The BCP may not be appropriately communicated to staff and key staff may not be aware of their roles in the plan.
6. The BCP may not be in a suitable location to allow it to be put into effect in the event of an emergency situation.
7. Staff contact details may not be kept up to date in the BCP.

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 sample testing and therefore will not provide assurance over all business continuity aspects within the College. We are reliant on the honest representation by staff and timely provision of information as part of this review.



APPENDIX IV: 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.

GEMMA MACGREGOR	VICE PRINCIPAL (OPERATIONS)
BRENDAN HALL	BUSINESS AND PROJECTS OFFICER
AMY GARRICK WRIGHT	ESTATES TECHNICIAN



APPENDIX V: 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, HEAD OF DIGITAL,
RISK AND ADVISORY SERVICES - SCOTLAND**

+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