Item: 8.2

Monitoring and Audit Committee: 9 June 2022.

Internal Audit Report: Business Continuity.

Report by Chief Internal Auditor.

1. Purpose of Report

To present internal audit on procedures and controls relating to business continuity.

2. Recommendations

The Committee is invited to note:

2.1.

That Internal Audit has undertaken an audit of processes and controls relating to business continuity.

2.2.

The findings contained in the internal audit report, attached as Appendix 1 to this report, relating to processes and controls relating to business continuity.

It is recommended:

2.3.

That the Committee review the audit findings to obtain assurance that action has been taken or agreed where necessary.

3. Background

3.1.

Business continuity considers the Council’s capability to continue services, at pre-defined acceptable levels, following a disruptive incident.

3.2.

Business continuity planning is intended to achieve the minimum of disruption to the delivery of business-critical systems from the effects of major failures or disasters. A business continuity plan should provide a well-defined set of procedures to be followed in order to maintain business-critical delivery and to achieve recovery from such events.

3.3.

The objective of this audit was to confirm that there is effective business continuity planning in place, that roles and responsibilities of Officers are documented and readily available and that appropriate monitoring and reporting mechanisms are in place.

4. Audit Findings

4.1.

The audit provides adequate assurance that the processes and procedures relating to business continuity are well controlled and managed.

4.2.

The internal audit report, attached as Appendix 1 to this report, includes nine medium priority recommendations within the action plan. There are no high-level recommendations made as a result of this audit.

4.3.

The Committee is invited to review the audit findings to obtain assurance that action has been taken or agreed where necessary.

5. Corporate Governance

This report relates to the Council complying with governance and scrutiny and therefore does not directly support and contribute to improved outcomes for communities as outlined in the Council Plan and the Local Outcomes Improvement Plan.

6. Financial Implications

There are no financial implications associated directly with the recommendations in this report.

7. Legal Aspects

Complying with recommendations made by the internal auditors helps the Council meet its statutory obligations to secure best value.

8. Contact Officers

Andrew Paterson, Chief Internal Auditor, extension 2107, email andrew.paterson@orkney.gov.uk.

Peter Thomas, Internal Auditor, extension 2135, email peter.thomas@orkney.gov.uk.

9. Appendix

Appendix 1: Internal Audit Report: Business Continuity.

Appendix 1

Orkney Islands Council

Internal Audit

Audit Report	
Business Continuity	
Draft issue date:	**29 April 2022**
Final issue date:	**12 May 2022**
Distribution list:	Safety and Resilience Manager Interim Head of Service for Property, IT and Facilities Corporate Director for Neighbourhood Services and Infrastructure Corporate Director for Strategy, Performance and Business Corporate Director for Education, Leisure and Housing Chief Officer for Orkney Health and Social Care Partnership Corporate Director of Finance, Regulatory, Marine and Transportation Services Head of Human Resources and Organisational Development Interim Chief Executive

Contents

Audit Opinion

Based on our findings in this review we have given the following audit opinion.

Adequate	**Some improvements are required to enhance the effectiveness of the framework of governance, risk management and control.**

A key to our audit opinions and level of recommendations is shown at the end of this report.

Executive Summary

Our audit provides adequate assurance that business continuity management and controls within the Council are being addressed with some areas of good practice being evident, including:

- The Council's Business Continuity Management Policy, Major Emergency Plan and Care for People Plan.
- Detailed Business Impact Analysis carried out throughout the Council.
- Support provided by the Safety and Resilience Team to Services.

Although progress has been made towards business continuity planning within the Council, further developments are needed for planning to be comprehensive and for robust continuity arrangements to be in place.

The report includes 9 recommendations which have arisen from the audit. The number and priority of the recommendations are set out in the table below. The priority headings assist management in assessing the significance of the issues raised. These recommendations have been made to assist the Council in the further development of its business continuity planning.

Responsible officers will be required to update progress on the agreed actions via Pentana Risk.

Total	High	Medium	Low
9	0	9	0

The assistance provided by officers contacted during this audit is gratefully acknowledged.

Introduction

Business continuity considers the Council's capability to continue services, at pre-defined acceptable levels, following a disruptive incident.

Business continuity planning (BCP) is the process of creating systems of prevention and recovery to deal with potential threats to the Council in delivering its services.

Business continuity planning is intended to achieve the minimum of disruption to the delivery of business-critical systems from the effects of major failures or disasters. A BCP should provide a well-defined set of procedures to be followed in order to maintain business-critical delivery and to achieve recovery from such events. A failure to develop effective BCPs could result in a haphazard approach being adopted should a BCP event occur. This could increase exposure to a range of operational, financial and reputational risks.

This review was conducted in conformance with the Public Sector Internal Audit Standards.

Audit Scope

The scope of the audit included:

- Ensuring that roles and responsibilities of Officers, the Senior Management Team (now called the Corporate Leadership Team) and the Extended Corporate Leadership Team, in relation to business continuity planning are documented, readily accessible and understood.
- Reviewing whether there is effective business continuity planning in place, that these are up to date and cover all key systems operating within the Council.
- Ensuring that appropriate monitoring and reporting mechanisms are in place to provide the Senior Management Team (now Corporate Leadership Team) and Members, with updates on any issues in relation to business continuity planning and, where appropriate, whether these are linked to the Council's risk register.

Background

Business continuity management (BCM) may be defined as the advance planning and preparation undertaken to ensure that an organisation will have the capability to operate its critical business functions during emergency events.

The Council's Business Continuity Management Policy (the Policy) was considered by the Council's Policy and Resources Committee on 25 September 2018 and approved by the Council on 9 October 2018.

Around the time of the review of the Policy, a substantial change in how the Council discharges its responsibilities for effective business continuity planning took place. The existing approach of Service Area Recover Plans (SARPs) was replaced with a process of developing Business Impact Analysis (BIAs) and then Business Continuity Plans (BCPs). This bringing the Council's business continuity planning in line with guidance from the Business Continuity Institute's Good Practice Guidelines.

Good progress had been made in the development of BIAs throughout the Council, however progress towards each of the lifecycle stages was significantly impinged during the current pandemic. Although the Council and its partners have generally responded well to the challenges of the pandemic, resources within both the Safety and Resilience team and also Services needed to be prioritised towards responsive work following the declaration of a major emergency.

Achieving full compliance to the Business Continuity Institute's good practice guidance would be a significant exercise for the Council which would require appropriate resourcing.

The Policy requires Executive Directors/Chief Officer and respective Heads of Service to have Business Continuity Plans in place, and that these plans are reviewed and updated biennially and exercised, as a minimum annually.

Section 8 of the policy states that the Civil Contingencies Act 2004, Section 2 (1)(c) places a duty on all Category 1 responders, (including Local Authorities), to maintain plans for the purpose of ensuring, so far as is reasonably practicable, that if an emergency occurs the person or body is able to continue to perform his or its functions.

The Policy requires the Council to maintain a Business Continuity Management System which will have regard to guidance within the Business Continuity Institute Good Practice Guidelines, and the Preparing Scotland – Having and Promoting Business Resilience guidance notes. Both frameworks, together with other industry systems such as ISO 22301:2019 have different nuances, however, in general terms, adherence to one framework will largely provide adherence to each of the other methodologies.

The Business Continuity Institute Good Practice Guidelines has six essential life cycle stages, as shown in figure 1.

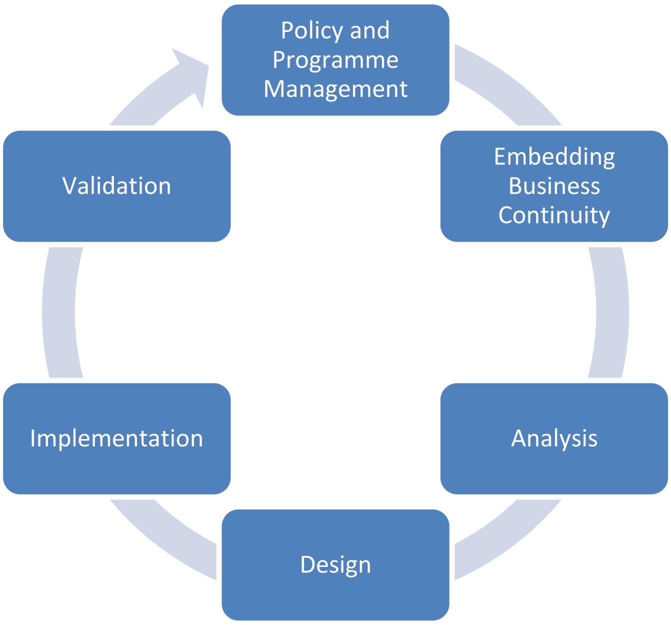
Policy and Programme Management
Embedding Business Continuity
Analysis
Design
Implementation
Validation

Figure 1

Stages

1. Policy and Programme Management - is the stage of the BCM lifecycle that establishes the organisation's policy relating to business continuity and defines how it should be implemented, through an ongoing cycle of activities within the business continuity programme.

2. Embedding - is the stage of the BCM lifecycle that defines how to integrate business continuity practice into business-as-usual activities and the organisation’s culture.

3. Analysis - is the stage of the BCM lifecycle that reviews and assesses an organisation to identify its objectives, how it functions, and the constraints of its operating environment. The main technique used to analyse the organisation is the Business Impact Analysis. A risk and threat assessment should also be undertaken at this stage.

4. Design - is the stage of the BCM lifecycle that identifies and selects solutions to determine how business continuity can be achieved during disruption.

5. Implementation - is the stage of the BCM lifecycle that implements the solutions agreed in the Design stage by establishing a response structure and developing plans. Business continuity plans should include details of the priorities, procedures, responsibilities and resources required to manage an incident and return the organisation to pre-agreed acceptable levels of service within the planned time frames.

6. Validation - is the stage of the BCM lifecycle that confirms the business continuity programme meets the objectives of the policy and that the plans in place are effective. The goal should be continual improvement of the programme and an enhanced level of organisational resilience.

Our review, and report has been structured around these six life cycle stages.

Orkney Islands Council makes up part of the Highlands and Islands Local Resilience Partnership (HILRP), the overarching group that ensures good partner and agency working in the region.

Audit Findings

1.0 Policy and Programme Management

1.1 The Council’s existing Business Continuity Management Policy was considered by the Policy and Resources Committee on 25 September 2018 and approved by Full Council on 9 October 2018.

1.2 A revised Business Continuity Management Policy has been largely prepared, with some review for changes in job roles and current practice, however at the time of our audit review, awaits update to job role responsibilities once the current Council restructure is complete.

1.3 The revised Business Continuity Management Policy is scheduled to be presented for consideration to the next meeting of the Policy and Resources Committee to be held on 21 June 2022.

1.4 The Council’s Business Continuity Management Policy requires review biennially. However, because the policy is scheduled for the next meeting of the Policy and Resources Committee a recommendation has not been made for this to take place.

1.5 A formal debrief report to the Council’s COVID-19 response up to March 2021 (the debrief) has been produced by the Council’s Safety and Resilience Manager.

1.6 The debrief identifies many findings, our review only considers those findings relating to Business Continuity Planning.

1.7 The debrief states that the Strategic Incident Management Team (SIMT) considered that:

- ➢ The Major Emergency Plan was fit for purpose and would require amendment to include the use of Community Resilience Groups and the Incident Support team.
- ➢ The Care for People Plan had been instrumental in setting up arrangements for the Humanitarian Assistance Centre but would require amendment following lessons learned across Scotland, and the UK.
- ➢ The Business Continuity Plan requires further refinement. The enormity of this incident had tested all resources and services nationally and the Council should build learning into the next iteration of the Plan. The use of Service Operational Recovery Teams was positive across most Services within the Council.

1.8 We understand that, at the time of our audit, the Council's Major Emergency Plan was scheduled for review shortly and that revision of the Care for People Plan had progressed to the stage of awaiting final sign off.

1.9 The Incident Management Team (IMT) similarly thought that plans were fit for purpose, recognising the fast-changing environment and demands made of the respective services responding to national guidance.

1.10 Representatives of Community Resilience Groups highlighted that existing Community Plans were inadequate to deal with the pandemic.

1.11 The Council was awarded winner of the Community Involvement category of the 2021 Local Government Chronical (LGC), the judges commenting that "After excelling during the rigorous judging process, Orkney Islands Council emerged as the winner of Community Involvement. Working in, with and for communities during COVID and beyond made an immediate difference on a daily basis despite the unrivalled geographical challenges they faced. Innovative, creative, willing to lead, supporting each other and creating a legacy which will continue to change lives on the (Orkney) mainland and islands forever. All this while being the smallest council in Scotland. Very well done. An example of local government at its very best!"

1.12 One of the recommendations relating to business continuity within the debrief was that the Council should develop a contact directory for all staff.

Recommendation 1

1.13 Another recommendation relating to business continuity within the debrief was that the Council should incorporate business continuity into its remote working policy.

Recommendation 2

1.14 Further recommendations relating to business continuity within the debrief are that:

- ➢ The Major Emergency Plan should include the requirement for weekly briefings with Members.
- ➢ The Major Emergency Plan should include the Incident Support Team and Community Resilience Groups.
- ➢ The Council's Care for People Plan should be reviewed to incorporate lessons learned from the challenges faced from the COVID-19 pandemic.

- The Council's business continuity arrangements should be reviewed to incorporate lessons learned from the challenges faced from the COVID-19 pandemic.
- Community Councils should lead on the creation of or amendment to Community Resilience Plans.

1.15 Recommendations made within the debrief relating to business continuity should be completed.

Recommendation 3

1.16 On 6 October 2021, a tabletop exercise was carried out within the Council based on the "Exercise in a Box" developed by the National Cyber Security Centre following the ransomware attack /infection that had shut down the entire IT system of the Scottish Environment Protection Agency (SEPA). The overall aim of the exercise was "to expose senior management to the issues that result from a ransomware attack".

1.17 Our review considers the outcomes from the Exercise in a Box where it relates to business continuity planning. This audit does not consider specifically the Council's resilience to cyber security.

1.18 The exercise interjects, and the presentation delivered by Robbie MacDonald of SEPA resilience identified the following issues:

- That training and testing/exercising of the business continuity plans make a significant difference to our ability to respond.
- To explore the use of holding critical business continuity plans, either in hard format or stand-alone digital format.
- That Services need to understand what resources they require to run their service off-line, and this should be reflected in their business continuity plans.
- Robust business recovery plans need to focus on critical front-line functions, such as ongoing statutory functions, payroll, and internal and external communications.
- That business recovery plans should include the possibility that all stored data subject to the ransomware attack will not be recoverable. Vital records needed for continuation of services should be included within business continuity planning.
- That business recovery plans should include a recognition that the recovery may take a considerable time and resource. That business recovery plans should be exercised regularly by senior managers responsible for their respective area of business and that these plans include the possibility of a complete loss of IT services for a considerable time.
- To develop a crisis communications plan, both internal and external.
- To be aware that concurrent incidents may occur and that this should be reflected in business continuity planning.

1.19 Matters identified from the Exercise in a Box should be included within the Council's business continuity planning.

Recommendation 4

2.0 Embedding

2.1 Following a meeting of the Council's Senior Management Team on 10 July 2018, work commenced on the compilation of Business Impact Analysis across each Directorate.

2.2 The process being that managers would compile and assess the BIAs for their respective activities, these would then be reviewed and signed off by the respective Head of Service before, in turn being delivered to the Executive Director/Chief Officer. Once satisfied that they had been completed and graded appropriately the BIAs would then be passed onto the Civil Contingencies Officer (this position has now been replaced by the Safety and Resilience Officer). Thereafter these would be re-ordered in terms of priority and passed to the Senior Management Team (now Corporate Leadership Team) for final sign off prior to the next phase of work commencing.

2.3 The assistance of the Safety and Resilience Officer was offered throughout, and a number of group and individual sessions were delivered. These sessions included, inter alia, presentation of a well-structured flowchart to follow in carrying out business impact analysis.

2.4 The Council's BIA provided to internal audit is dated 28 January 2020.

2.5 The Council's BCM policy is that, as a minimum standard, BIAs will be reviewed biennially or following a significant change.

2.6 We understand that a process to review BIAs has commenced and is in its early stages. Whilst it is recognised that review of BIAs throughout the Council is a substantial exercise the Council should aim to adhere to its policy.

2.7 Prior to the review of BIAs that commenced in 2018, its previous review took place in 2010. Should BIAs not be regularly reviewed, they will not be updated to internal changes or to wider development of good practice across the profession.

2.8 It is therefore recommended that the review of BIAs across the Council be progressed.

Recommendation 5

3.0 Analysis

3.1 The Council's corporate BIA is considered to be comprehensive and well structured. The corporate BIA considers 1397 activities throughout the Council.

3.2 The corporate BIA pays some cognisance to risk assessment, providing a scoring system to evaluate 7 types of risk namely risks to: loss of life or injury, legal or regulatory duties impact on the environment, failure of emergency response, reputational, finance, and major impact to the Council's strategic priorities.

3.3 Compliance to the Business Continuity Institute Good Practice Guidelines requires threat and risk assessment to be carried out to all council services.

3.4 It is therefore recommended that service risk and threat assessments be developed throughout the Council.

Recommendation 6

4.0 Design

4.1 The Corporate BIA details the solution to potential threats to each of the 1397 activities detailed within the list.

4.2 The BIA also details the maximum tolerable period of disruption, and also the recovery time objective for the 1397 activities.

5.0 Implementation

5.1 The Council has carried out much work to identify the risk of disruption to all 1397 activities and in detailing their respective solution.

5.2 Services are only at an early part of the stage of developing and implementing the outcomes from the Design stage in establishing a response structure and developing clear, concise and accessible business continuity plans.

5.3 There are several examples where Service business continuity plans could not be provided to internal audit. In instances where the business continuity plan could be provided, there were several examples where these did not contain contact details, or provided contact details of former employees, did not provide clarity to how the plan would be engaged, or did not define respective authority levels.

5.4 It is recommended that each Directorate maintains a log of each business plan it holds together with the location of its, network, stand alone and hard copy version. The log should be used to identify gaps in business continuity planning within the Directorate.

Recommendation 7

5.5 Business continuity plans should be easily accessible, for example on the Council's intranet, relevant staff should be advised of the location of the plans in order that they are aware of their content.

Recommendation 8

6.0 Validation

6.1 The Council's Major Emergency Plan requires its review and testing to take place at least once every three years.

6.2 The Council's resilience to major emergency has been severely tested from the challenges of the COVID-19 pandemic. The debrief review has identified many valuable lessons learned from the Council's response to the pandemic.

6.3 Processes should be developed to capture findings from future test exercises so that they are incorporated into business continuity plans, where identified.

Recommendation 9

Action Plan

Recommendation	Priority	Management Comments	Responsible Officer	Agreed Completion Date
1) The Council should develop a contact directory for all staff		Agreed. Work on this is underway	Head of Human Resources and Organisational Development	30 September 2022
2) The Council should incorporate business continuity into its remote working policy.		Agreed. A policy on remote working will be developed and this will take account of potential business continuity issues.	Head of Human Resources and Organisational Development	31 December 2022
3) The remaining recommendations relating to business continuity made within the debrief relating to business continuity should be completed.	Medium	Agreed. The remaining recommendations from the debrief to business continuity planning should be implemented by Services supported by the Council's Safety and Resilience Manager and Team.	Corporate Directors/Chief Officer (supported by Safety and Resilience Manager).	31 December 2022
4) Matters identified from the exercise in a box should be included within the Council's business continuity plans.	Medium	Agreed	Corporate Directors/Chief Officer (supported by Safety and Resilience Manager).	31 December 2022
5) Existing Business Impact Analyses (BIAs) within the Council should be reviewed.	Medium	Agreed, Services were tasked with this activity in November 2021.	Corporate Directors/Chief Officer as per Business Continuity Policy	31 December 2022
6) Service risk and threat assessments should be developed throughout the Council.	Medium	Agreed	Corporate Directors/Chief Officer as per Business Continuity Policy	31 December 2022

7) Each Service should maintain a log of each business plan it holds together with the location of network, and hard copy version. The log should be used to identify gaps in Business Continuity Plans within the Service.	Medium	Agreed	Corporate Directors/Chief Officer	31 December 2022
8) Business Continuity plans should be easily accessible to Staff, for example on the Council’s intranet.	Medium	Agreed The structure for recording business continuity plans on the Council’s intranet will be developed.	Development by the Safety and Resilience Manager, ongoing maintenance is the responsibility of Services	31 September 2022
9) Processes should be developed to capture findings from future test exercises so that they are incorporated into business continuity plans where identified.	Medium	This is contained within the debrief process, such as that within Exercise in a box. Debrief report sent to the Corporate Leadership Team for approval and cascaded to Corporate Directors/Chief Officer for progression.	Safety and Resilience Manager	Already Completed The Debrief report has already been sent to the Corporate Leadership team. Its implementation will be an ongoing activity.

Key to Opinion and Priorities

Audit Opinion

Opinion	Definition
Substantial	The framework of governance, risk management and control were found to be comprehensive and effective.
Adequate	Some improvements are required to enhance the effectiveness of the framework of governance, risk management and control.
Limited	There are significant weaknesses in the framework of governance, risk management and control such that it could be or become inadequate and ineffective.
Unsatisfactory	There are fundamental weaknesses in the framework of governance, risk management and control such that it is inadequate and ineffective or is likely to fail.

Recommendations

Priority	Definition	Action Required
High	Significant weakness in governance, risk management and control that if unresolved exposes the organisation to an unacceptable level of residual risk.	Remedial action must be taken urgently and within an agreed timescale.
Medium	Weakness in governance, risk management and control that if unresolved exposes the organisation to a high level of residual risk.	Remedial action should be taken at the earliest opportunity and within an agreed timescale.
Low	Scope for improvement in governance, risk management and control.	Remedial action should be prioritised and undertaken within an agreed timescale.