Appendix 1. Executive Summary: Business Continuity

Conclusion: Limited Assurance

A Business Continuity system was purchased in 2020 but is only used in a very limited capacity within the Place Directorate to document and monitor business continuity plans making it difficult to track the Council's overall progress in improving its resilience, there is insufficient resource within Protective Services or Business Applications to rollout the Business Continuity system to more users, Protective Services do not have an adequate process for recording and monitoring Directorate/Service compliance with the corporate policy, there are critical services within the Council that do not have adequate or up-to-date business continuity plans, plans are not tested consistently, the Business Continuity Policy requires update, the available training improved, and the written procedures available for services on business continuity require review and expansion.

Background

The Civil Contingencies Act 2004 sets out specific duties for local authorities in relation to Business Continuity (for example to maintain business continuity plans and provide generic advice and assistance in connection with business continuity, including signposting to specialist services). An approved Business Continuity Policy is in place which was last updated in 2017. A Contingency Planning Officer (CPO), which is multidisciplinary in role, is in post within Protective Services and is responsible for facilitating the provision of business continuity advice and training to services. In addition, the role supports the response to business continuity incidents and has responsibility to establish a process for recording compliance with the corporate Business Continuity Policy. The Contingency Planning Group (referenced in the 2017 Business Continuity policy) which became the Risk & Resilience Group (as distinct from the current Strategic Risk and Resilience Group responsible for monitoring the Council's strategic risks) was responsible for monitoring compliance with the corporate policy and was chaired by the previous Waste Risk and Resilience Manager. The Risk & Resilience Group has not met since 2020. As noted in the Business Continuity Policy, Senior Management are responsible for ensuring business continuity plans are prepared for their Directorate / Service, tested, reviewed, critical activities at a service level have been agreed, and employees in their Directorate have received an appropriate level of awareness and training on the business continuity management process.

Summary of findings and recommendations

The following key findings and recommendations are highlighted, which have all been agreed by Management:

- Although a business continuity system was procured in 2020, its implementation was impacted by the Covid Pandemic and the Council restructuring which occurred around that time, and its roll out is limited to a small number of pilot users within the Place Directorate. The business case and implementation plan were insufficiently developed post-procurement. The Health Safety and Resilience Team service review has identified there is insufficient resource within their service. *Management will review resource required to support an implementation of a business continuity system and ongoing support by* ***September 2025****.*
- A number of critical areas do not have adequate or up-to-date business continuity plans, or in some cases have no plans. Services with no plans or recently created plans have not undergone testing of their plans. *Chief Officers will ensure the creation of appropriate business continuity plans by* ***December 2025*** *and ensure that these are thereafter periodically reviewed, updated and tested.*
- The Health Safety and Resilience Team do not have an adequate process for recording and monitoring Directorate/Service compliance with the corporate policy, including the monitoring and review of Business Continuity Plans and the reporting of compliance to management. *Management will ensure that appropriate monitoring with the corporate policy is in place, and this will include reviewing the level of resource assigned to support this by* ***September 2025****.*

- There is no formal Digital Services Annual Business Continuity Testing Programme in place. *Management will implement an Annual Testing Programme by **September 2025**.*
- There is no appropriate forum/group in place for Business Continuity Leads to meet, at least annually, to discuss business continuity with other service leads and Protective Services officers. *Management will host a forum with Business Continuity Leads from each service at least annually to update knowledge on business continuity and support Contingency Planning in recording and monitoring Directorate/Service compliance with the corporate policy by **October 2025**.*
- The Business Continuity Policy is overdue for review; however a review is currently underway. This means the Council's approach has not recently been endorsed at a senior level. *Management will ensure that the policy is reviewed and updated by **June 2025**.*
- The guidance provided to services requires review and standardisation, guidance further developed for Business Continuity Leads, and the training available enhanced (e.g. through development of an e-Learning module). *Management will update the business continuity guidance and implement a business continuity e-learning module by **October 2025**.*

Recommendations Grade	High	Medium	Low	Total
Current Report	2	5	-	-
Prior Report (2022)	2	-	-	-

Materiality - The recent cyber-attack on Western Isles Council is anticipated to cost the Council £1m and the cyber-attack on SEPA is reported to have cost the organisation £5.5m. The Council would be liable, at minimum, to pay the policy excess following the loss or significant damage to any Council building (e.g. following a fire or flood) and likely further recovery costs. Shortages of resources, such as fuel or power, would result in the Council not being able to deliver services as expected, likely resulting in increased costs for the Council.

Headlines

Objectives	Conclusion	Comments
1. Business critical services across the Council have been identified and processes are in place to ensure that business continuity plans for those areas remain up-to-date, aligned with service delivery requirements and continue to be fit for purpose.	**Limited Assurance**	Critical services identified include the Contact Centre, Child Protection and Vulnerable Children's Services, Education, and the Health and Social Care Partnership. The Council's Business Continuity Policy was approved in 2017 and requires update to take into account the increased cyber security risk, the systems to be prioritised in the event of a severe cyber-attack, the learning from the Covid response and the Council's current organisational structure (update in progress). The Health Safety and Resilience Team do not have an adequate process for recording and monitoring Directorate/Service compliance with the corporate policy. Additionally, the guidance and training provided to services requires review and improvement. Delivering this may require additional resource within the team as identified by the service review. A system was purchased in 2020 to enable services to record their business continuity plans electronically, but it has not been implemented across the Council - current users are limited to a small number of pilot users within the Place Directorate. Therefore, it is not possible to get an accurate picture of what plans are in place or if they are up-to-date without contacting each service manager individually. The implementation of the business continuity system was not adequately resourced and the rollout of the application to other services has stalled. It was identified during the audit from the sample of services reviewed in the Place Directorate, Children, Young People and Partnerships, and Social Care that a number of critical areas do not have adequate or up-to-date Council business continuity plans, or in some cases have no plans.
2. A programme of testing has been developed to validate, over time, the effectiveness of business continuity plans and solutions.	**Limited Assurance**	As noted above, many services do not have up-to-date business continuity plans. Some services within Place Directorate have been updating their business continuity plans this year, but as these plans have only recently been updated, they have not yet been tested. Digital Services have an up-to-date Cyber Response Plan, Playbooks for different types of potential cyber-attack, and undertake business continuity exercises. There is no Annual Business Continuity Testing Programme for formally testing specific aspects of systems and ensuring that all relevant system specific documentation is up-to-date.
3. Following testing, changes and improvements have been implemented, where required.	**Limited Assurance**	As noted above, business continuity plans have not been appropriately developed or tested across the Council. However, Digital Services were able to provide evidence of business continuity exercises carried out and lessons learned from their exercises. The lessons learned have contributed to their Cyber Security Action Plan and updated business continuity policies.

Areas where expected controls are met/good practice

No.	Areas of Positive Assurance
1.	Digital Services created a Cyber Security Action Plan in 2022 following a number of high-profile cyber-attacks on public sector organisations and have improved the Council's resilience following the completion of the majority of the identified actions. This included the implementation of a password manager, vulnerability management software, improving the Council's backup arrangements to include cloud backup, and procuring a cyber incident response retainer to support the Council in the event of a cyber-attack.
2	The Council is moving more of its applications to cloud based 'software as a service' solution each year, which improves the Council's digital resilience.
3.	The importance of business continuity planning, particularly in relation to the impact of a cyber-attack, was reinforced in detail to senior management at Leadership Forum events in June and September this year and relevant guidance was issued following this event.
4.	The procurement of a business continuity system has been undertaken and there is an option to extend the contract until December 2030, meaning this could be rolled out across the Council provided the project was suitably resourced.
5	Following NHS Lothian processes and procedures, Council delivered Health and Social Care Partnership Services have prepared plans for their services outlining management arrangements, key suppliers, buildings, resources, and how actions should be documented if a significant event requiring invocation of the plan were to occur. It was advised that the Plans have been made available in a section of the NHS Lothian network that will still be accessible if the main network is offline due to, for example, a cyber-attack. Business continuity within Council Services delivered by the Health and Social Care Partnership is monitored and reviewed by local NHS resilience arrangements, including: - Daily STAT PREP meetings to record system, service and staffing pressures. - Critical Services list to reallocate staffing to areas under increased demand. - Virtual control room and processes in place and routinely tested. - Twice annual assurance reporting on resilience and continuity. - NHS led annual exercises both tabletop and internal. - Executive level resilience support provided by Executive Business Manager.
6	The Development of Business Continuity plans are the function and responsibility of each Directorate / Service. Business Continuity is a standing item on the Children, Young People and Partnerships and HSCP DMT. Children, Young People and Partnerships have sought support from a neighbouring authority to assist in developing their business continuity processes. Whilst internal support has been sought to develop service specific business continuity plans, the Executive Director was informed there was no capacity within the Place Directorate to provide support in drafting their business continuity plans. An external consultant has been appointed to undertake this work which the Executive Director has been advised is due to be complete by end of March 2025.