Internal Audit Report
Business Continuity 2023/24

Draft report: 31 July 2024
Final report: 3 September 2024
Last audited: September 2013 (Satisfactory assurance opinion)

Audit Objective	The business continuity approach and ownership is documented, with guidance and templates in place and that third parties provide assurances.

Assurance Opinion	
Reasonable	There is a generally sound system of governance, risk management and control in place. Some issues, non-compliance or scope for improvement were identified which may put at risk the achievement of objectives in the area audited.

Number of Actions

Priority	Joint	South	Vale	Reference
Priority 1	1	-	-	1
Priority 2	2	-	-	2 and 3
Priority 3	-	-	-	-
Total	**3**	**-**	**-**	**Appendix 1**

Key Risks Reviewed

- Council services not being provided could result in a financial penalty.
- A disaster could result in additional costs being incurred to provide additional resources to continue service provision to the public.
- Officers not executing the business continuity plan could result in reputational damage.
- Business continuity plan not communicated to officers appropriately could cause services to stop.

The audit scope included:

Objective		Audit Scope
1	Ownership and responsibility	• Ownership and responsibility for business continuity management is clearly defined and documented. • Training is provided all officers who have responsibility in the business continuity process.
2	Strategy and procedures	• An up-to-date strategy is in place, which is adequately detailed and available to officers. • Up to date templates, guidance and procedures are in pace and available to officers.
3	Business continuity approach	• The business continuity approach in place is: - fit for purpose. - regularly reviewed. - kept confidentially. - supported with appropriate documentation. - regularly tested.
4	Third parties	• Third party contractors have adequate business continuity processes in place.

Key Findings		
Objective		**Audit Scope**
1	Ownership and responsibility	• The corporate programmes team is responsible for the administration and management of business continuity activities and the team is fully resourced. • The business continuity strategy documents the roles and responsibilities for business continuity, which is available to all officers on Jarvis. • A crisis response team (CRT), comprising the strategic management team is set up to invoke the business continuity approach when an emergency occurs.
2	Strategy and procedures	• The business continuity strategy was last reviewed and approved in August 2023. The contents of the strategy are aligned to the gov.uk 'How prepared are you?' best practice guidance. • Business continuity guidance and templates, such as business process map, business risk register and business resilience plan, are up to date and available to all officers on Jarvis.

3	Business continuity approach	• The business continuity approach is incorporated into the business continuity strategy. It is fit for purpose and in line with best practice.
		• Per the business resilience plan (BRP) review schedule, plans were due for review in April 2024; however, we confirmed that all eight plans need updating.
		• Each service area has their own business risk register which identifies risks that could prevent the service from achieving the business resilience plan. All eight business risk registers need updating.
		• The annual business continuity testing programme is determined based on date of last exercise, organisation risk, and business impact; however, the methodology used to identify testing exercises is not documented.
		• The testing programme for 2024/25 includes six exercises to be undertaken by either the Corporate Programmes team or Capita:
		  ○ The three Capita-led exercises test the high-risk areas of internal/external penetration of Capita IT systems and testing of the Capita disaster recovery plan. These exercises are performed annually, and the results are shared with the councils.
		  ○ The three council led exercises include a test of all parts of the BRP (tabletop exercise), call cascade, and National Cyber Security Centre (NCSC) exercise in a box (i.e., responding to a cyber-attack). Although added to the testing programme for 2024/25, these exercises have not been undertaken in at least three years. Consequently, we are unable to review any completed council-led exercises.
		• As noted above, a tabletop exercise has not been performed in the last three years. Additionally, a tabletop exercise for 2024/25 has not been decided, therefore testing procedures are not established and critical services are not identified. Once the tabletop exercise is complete, it is recommended that the exercise procedure, outcomes, and lessons learned are documented.

4	Third parties	• Third party agreements are in place for outsourced council services (e.g., Capita, Biffa Waste and Greenwich Leisure Limited (GLL)) and we are satisfied that third party business continuity plans are provided in line with the agreements. • Capita provides IT services to the councils and as part of the service, Capita are required to undertake annual testing on their disaster recovery plan and the internal/external penetration of the IT systems. The results of the testing are provided to the councils for review and comment. • South and Vale regularly attend resilience groups attended by other authorities in the Thames Valley area, with the aim of collating and sharing learnings, identify best practice, and develop and embed multi-agency response arrangements throughout the area.

Appendix 1 - Detailed Findings and Management Actions

Obj3: Business continuity approach			Priority 1
1. Business resilience plan			
Findings	**Management Actions**	**Due Date**	**Action Owner**
It is best practice for service areas to review and update their business resilience plan (BRP), process maps, and risk register on a regular basis. All nine BRPs need updating, as information such as BRP processes and contact details are outdated. Due to recent organisational changes some service teams are included in the incorrect BRP. All nine business process maps and risk registers are outdated. Examples of incorrect information include risk owner contact details and incomplete identification of risks.	a) Remind service areas to review and update their business resilience plan to ensure that: • teams are in the correct service area's business resilience plan; • contact details are up to date; • BRP processes are up to date; and • business risk register is up to date. b) Document any contact with service teams and any necessary escalation actions required to ensure that the service area's business resilience plan documentation is kept up to date.	30 November 2024	Programmes Team Leader
Risk			
Contact details not being updated can result in officers are not being notified when a disaster occurs. Teams not being in the correct service areas can result in officers not being notified as the team can be missed in the call cascading process. Risk registers not regularly reviewed and updated could result in unidentified risks occurring preventing services from running during an emergency.			
Management Response			
Management actions are **Agreed** Thank you for this feedback, we agree the recommendations and proposed management actions. Management response: Programmes Service Manager			

Obj3: Business continuity approach			Priority 2
2. Testing programme methodology			
Findings	**Management Actions**	**Due Date**	**Action Owner**
When determining the areas to include in the annual business continuity testing programme, it is recommended that the methodology is documented. We were informed that a balanced approach is undertaken in determining the annual business continuity test programme as the following factors are considered: • when the area was last tested. • risk to the organisation. • business areas impacted. However, the methodology used to develop the testing programme for 2024/25, including a final list of exercises to be performed in the upcoming year is not documented. Consequently, it is difficult to confirm if all areas and exercises have been suitably considered for testing.	Document the methodology used to develop the annual the annual testing programme.	30 November 2024	Programmes Team Leader
Risk			
Not documenting the risk approach could result in some business continuity areas being missed and not tested.			
Management Response			
Management actions are **Agreed** The team will document the risk-based methodology for determining the future proposed testing approaches including why each testing approach has been identified. Management response: Programmes Service Manager			

3.4

Agenda Item 9

Page 34

Obj3: Business continuity approach			Priority 2
3. Annual business continuity testing programme			
Findings	**Management Actions**	**Due Date**	**Action Owner**
Exercises should be undertaken regularly, and in line with the business continuity testing programme. Exercises should be fully documented, including a review of lessons learned. The testing programme for 2024/25 includes six exercises to be undertaken by either the Corporate Programmes team or Capita. The three council-led exercises include a test of all parts of the BRP (tabletop exercise), call cascade, and National Cyber Security Centre (NCSC) exercise in a box (i.e., responding to a cyber-attack). Although added to the testing programme for 2024/25, these exercises have not been undertaken in at least three years. Consequently, we are unable to review any completed council-led exercises. Additionally, a tabletop exercise for 2024/25 has not been decided, therefore testing procedures are not established and critical services are not identified. Once the tabletop exercise is complete, it is recommended that the exercise procedure, outcomes, and lessons learned are documented.	a) Decide upon a tabletop exercise and add to the 2024/25 testing programme. Once completed, establish testing procedures, and identify critical services. b) Undertake testing exercise. c) Establish a process to capture results and lessons learned from completed exercises.	30 November 2024	Programmes Team Leader
Risk			
The councils are unprepared for some business continuity scenarios. Weaknesses in the business resilience plan may go undetected. Recurrent control weaknesses are not recorded and remedied.			
Management Response			
Management actions are **Agreed** Thank you for this feedback, we agree the recommendations and proposed management actions. Management response: Programmes Service Manager			

3.4

Agenda Item 9

Page 35

Appendix 2 - Internal Audit Definitions

Overall Assurance Definitions	
Substantial	A sound system of governance, risk management and control exists, with internal controls operating effectively and being consistently applied to support the achievement of objectives in the area audited.
Reasonable	There is a generally sound system of governance, risk management and control in place. Some issues, non-compliance or scope for improvement were identified which may put at risk the achievement of objectives in the area audited.
Limited	Significant gaps, weaknesses or non-compliance were identified. Improvement is required to the system of governance, risk management and control to effectively manage risks to the achievement of objectives in the area audited.
No Assurance	Immediate action is required to address fundamental gaps, weaknesses or non-compliance identified. The system of governance, risk management and control is inadequate to effectively manage risks to the achievement of objectives in the area audited.

Categorisation of Actions	
In addition to linking findings to the corporate risk registers, it is important that management know how important the required action is to their service. Each action has been given a priority rating at service level with the following definitions:	
Priority 1	Findings that are fundamental to the integrity of the service's business processes and require the immediate attention of management.
Priority 2	Important findings that need to be resolved by management.
Priority 3	Finding that requires attention.