Business Continuity

City of York Council

Internal Audit Report 2020/21

Business Unit: Emergency Planning Unit
Responsible Officer: Director of Environment, Transport and Planning
Service Manager: Emergency Planning Manager
Date Issued: 26 November 2021
Status: Final
Reference: 11060/007

	P1	P2	P3
Actions	**0**	**3**	**2**
Overall Audit Opinion	Reasonable Assurance		

Summary and Overall Conclusions

Introduction

Business continuity is the ability of an organisation to continue delivering services at acceptable, predefined capacity levels and timeframes during disruptive events. Under the Civil Contingencies Act 2004 the Council is defined as a Category 1 responder and has a responsibility to ensure it can continue delivering some services during an emergency, so far as is reasonably practicable. The Act also requires that the Council maintain plans in order to facilitate its response, provide advice to the public and assess the risk of an emergency occurring.

The Chief Operating Officer has overall responsibility for ensuring that the Council has business continuity plans. However, responsibility for co-ordinating the plans as a central resource is undertaken by the Emergency Planning Unit (EPU). Production, ownership and review of the plans is the responsibility of each service and it is up to senior managers within each directorate to ensure that key services are maintained during an incident.

Objectives and Scope of the Audit

The purpose of this audit was to provide assurance to management that procedures and controls within the system ensure that:

- Suitable guidance is available and training is provided to plan owners responsible for producing business continuity plans.
- The EPU effectively and efficiently monitors, assesses and reports on business continuity plans' compliance with legislation, internal requirements and good practice.
- Suitable governance arrangements have been established for business continuity management within the Council.

The audit did not consider the production of individual service plans or provision of services by individual directorates because this is a responsibility of each directorate and outside the scope of the EPU. The audit did not assess the Council's response to the coronavirus pandemic or the activation of individual plans during the pandemic.

Although the Council's Incident Management Handbook only provides guidance for emergency planning, a review of the handbook was included in the audit scope because it had recently undergone significant revision. The review findings are included at appendix 1.

Key Findings

Overall, the EPU provides a wide variety of support, guidance and informal training to business continuity plan owners across the Council. Nevertheless, a number of control gaps were identified in existing arrangements during the audit. Much of the support provided by the service is reliant on the dedication and expertise of a small number of individuals within the EPU. Two of the three members of the EPU have recently left the Council, which may affect the EPU's ability to provide support and advice if they are not replaced. Plans are in place

for a shared service arrangement with North Yorkshire County Council, which will provide resilience and expertise in business continuity to the EPU. The arrangement will run for an initial 18-month pilot until 31 March 2023, with a final decision on the arrangements expected in September 2022.

The EPU has several guidance documents related to business continuity in place. The Council's business continuity policy records governance arrangements for business continuity management within the Council and outlines decision-making responsibilities. However, the policy does not identify how the multiple directorate-level business continuity plans should be co-ordinated and many of the roles and responsibilities listed are now outdated. Instead, the directorate-level plans themselves discuss the co-ordination of the service-level plans. An analysis of EPU-listed plan owners confirmed that all those with delegated responsibility for the plans were in suitably senior positions to enable them to enact their duties.

When the business continuity policy, associated templates and guidance provided to plan owners were reviewed, it was clear these documents had been developed with both ISO 22301:2012 (ISO) and the National Resilience Standards (NRS) in mind. Nevertheless, some inconsistencies were identified between these documents and the documents were sometimes at odds with ISO or NRS guidance. The policy itself has not been widely shared with plan owners because it was last updated in 2014. However, the templates and guidance are frequently circulated to all responsible officers and updated as part of various annual review procedures. Inconsistencies are detailed at appendix 2.

Annual reviews of all business continuity plans maintained by the Council are undertaken by service areas, with support from the EPU. The EPU confirms that the reviews are completed and it reports on completion to CMT. Testing of the plan review sheet reports to CMT found 93% of all Council plans were updated in the October 2020 annual review, and similar completion rates were seen in previous years' annual reviews. However, a small number of plans had not been reviewed for two annual review cycles.

Outside of the annual review, plan owners are reminded in EPU guidance documents to update their plans as and when internal or external structures or arrangements change. Review of a sample of plans found that they were consistently not updated by owners outside of the annual review. Where changes were made, the EPU was not informed of them and in a small number of cases plan owners had left the council without informing the EPU.

Optional induction and refresher training is provided to business continuity plan owners on request. Training provided is often tailored to the needs of individual plan owners, based on the professional expertise of EPU staff. The absence of documented training records and the collection of only discretionary feedback made it challenging to assess independently the quality or extent of training provided.

Exercising of business continuity plans is also used as a key method of training staff whilst assessing the functionality of plans. Although a spreadsheet of exercises undertaken since 2017 was maintained by the EPU, key information about the exercises' scope, outcomes and lessons learned was not recorded. Based on the information provided it appears all plans may have been tested at least once since 2017, though without scoping information this could not be confirmed. However, responsibility for exercising directorate and service area plans lies with the relevant directorates and service areas, not the EPU.

Overall Conclusions

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. Our overall opinion of the controls within the system at the time of the audit was that they provided Reasonable Assurance.

1. Guidance provided to responsible officers

Issue/Control Weakness	Risk
Inconsistences were identified in the variety of business continuity plan templates, policy and other guidance offered to officers responsible for business continuity within the Council.	Suitable guidance is not provided to those responsible for business continuity plans. Consequently, the plans may not be effective or comply with statutory requirements.

Findings

The Emergency Planning Unit (EPU) provides a range of guidance to officers responsible for business continuity management. This guidance includes the Council's business continuity management policy, the service-level and directorate-level business continuity plan templates, the business impact analysis template and the communications provided to officers during the annual review.

The EPU does not maintain a review schedule for the guidance provided and, where reviews take place, the process is not documented. The policy was last updated in 2014; the directorate-level plans and templates were last reviewed in February 2020 and the service-level plans, templates and business impact analyses were last reviewed in October 2020.

During the audit, the guidance provided to officers was reviewed collectively and against business continuity best practice advocated by ISO 22301 and the National Resilience Standards (NRS). A number of inconsistencies were noted between the documents and communications provided. In a few cases, only some of the guidance provided met the advocated best practice and occasionally, none of the guidance addressed these best practices. Further details of these inconsistencies and issues are included at appendix 2.

At the start of the audit, the EPU confirmed they were aware of some of the issues identified with the policy and that the current policy does not directly link with either the templates or other guidance provided. Due to the lack of available resources, the EPU has not yet been able to resolve these issues.

Agreed Action 1.1

The business continuity policy, templates and guidance will be reviewed and updated to ensure they are consistent with each other and follow current best practice. Once the review is complete, they will be circulated to responsible officers.	**Priority** 2 **Responsible Officer** Emergency Planning Manager **Timescale** 31 January 2022

2. Annual review of business continuity plans

Issue/Control Weakness	Risk
Service areas do not always update their business continuity plans as part of the annual review process. In a small number of cases, this has occurred for more than one annual review cycle.	Business continuity plans may not be up to date, which may lead to services being unable to respond effectively during an incident.

Findings

Although the Emergency Planning Unit (EPU) is not responsible for writing or maintaining the Council's business continuity plans, they support the services in reviewing the plans and confirm that annual reviews have taken place. Reviews of the service-level and directorate-level plans are expected to be undertaken annually. However, only the service-level review was completed in 2020-21 due to the impact of Covid-19 on resourcing. A record of which services have completed the annual reviews was maintained by the former Emergency Planning Officer.

The EPU was reporting the results of the annual review to Corporate Management Team (CMT), with updates on which services had or had not updated their business continuity plans. Analysis of annual review information for 2017-18 to 2020-21 identified two service areas that had not reviewed their plans for two consecutive review cycles. One other service area was recorded as being a new service in 2017 and did not yet have a business continuity plan. This was still the case in the 2020 review records. Follow up with the service during the audit confirmed that it had prepared a business continuity plan. In a number of instances, services had not provided an updated plan or had provided it late during the annual review cycle.

Agreed Action 2.1

EPU now attend CMT four times per year to provide updates on business continuity, providing more visibility for the service at Corporate Management Team (CMT). The policy review will clearly identify the responsibilities of council management for ensuring service areas review and maintain their business continuity plans.	**Priority** 3 **Responsible Officer** Emergency Planning Manager / CMT **Timescale** 31 January 2022

3. Plan updates outside of the annual review

Issue/Control Weakness	Risk
Business continuity plans are only updated by the responsible officers during the Emergency Planning Unit's (EPU) annual review. Plans are not updated following the activation of a plan.	Business continuity plans are incomplete or out of date. This could lead to the Council failing to meet statutory requirements, experiencing avoidable financial losses, or other harm during an incident.

Findings

In order for business continuity plans to be effective both ISO 22301 and the National Resilience Standards (NRS) expect the plans to be updated after significant organisational or external changes. Consequently, the EPU frequently reminds responsible officers across the guidance provided to them that the officers must regularly update their plans outside of the annual review and inform the EPU of changes they have made. However, the EPU does not require responsible officers to update their plans following a plan's activation.

Testing of a sample of ten service-level plans found that only one plan had recorded any new updates since the most recent annual review in October 2020, despite two further Covid-19 national lockdowns and a significant organisational restructure occurring. Moreover, in the one case where an update was recorded, the EPU was not informed about the updated business continuity plan.

In two of the ten service-level plans sampled, officers did not respond to requests for copies of their most recent plans. Thus, it remains unclear whether these officers are the correct contacts for their service-level plans. To assess this issue, a reconciliation was undertaken of the Council's staff leavers list for the 2020-21 financial year against the EPU's list of plan owners. Only one responsible owner was identified as having left the council following the most recent annual review of the plans. However, Human Resources subsequently confirmed a further two officers were no longer employed by the Council. Unless service areas inform the EPU of staff members leaving, there is currently no process for the EPU to find out about staffing changes.

Agreed Action 3.1

The policy review will include the requirement for plan owners to update their business continuity plans following a plan's activation.	**Priority**	3
	Responsible Officer	Emergency Planning Manager
	Timescale	31 January 2022

Agreed Action 3.2

The leavers' checklist will be revised to include a section on whether the leaver has	**Priority**	3

any business continuity responsibilities. The line manager will then review and update the relevant business continuity plan if changes are required.	**Responsible Officer**	Head of Human Resources
	Timescale	31 January 2022

Agreed Action 3.3		
Business continuity plans have been moved to a central, shared area of the V drive so that they are accessible to the EPU and all plan owners. Copies have also been uploaded to Resilience Direct.	**Priority**	3
	Responsible Officer	Emergency Planning Manager
	Timescale	Completed

4. Exercising of business continuity plans

Issue/Control Weakness	Risk
Business continuity plan exercises are not regularly conducted.	Gaps or faults with business continuity plans may not be identified until a major response is required.
Key details of exercises undertaken, such as what was tested, lessons learned, and resulting actions, are not recorded.	Lessons learnt from exercises are not considered in subsequent business continuity planning.

Findings

The Civil Contingencies Act 2004 requires all Category 1 responders, such as the Council, to maintain and exercise business continuity plans. Both ISO 22301 and the National Resilience Standards (NRS) state that in order for a business continuity plan to be considered effective, it must have been exercised to assess whether the plan functions as intended. Exercises should be conducted at planned intervals or after significant changes to the organisation or its operating environment.[1] In all cases, it is expected that the full extent of the plan will be exercised, albeit possibly over the course of an exercise schedule.

Business continuity plan owners are responsible for exercising their plans, although the EPU can provide support and advice for exercises if requested. In 2015, the Corporate Management Team (CMT) agreed to a minimum of two exercises to be held per directorate per year. A review of the evidence available found this requirement does not appear to have been met by all directorates. Assuming that the exercises listed by the EPU did cover all elements of the plans named within the scope of the exercise, it appears that all service-level and directorate-level plans have been exercised at least once, mostly in 2017.

An exercise schedule was started in 2017 by the EPU to record exercises undertaken. This was last updated in 2019 because the Covid-19 pandemic prevented exercises in 2020-21. The quality of information recorded on the schedule varied significantly. Key details, such as what was tested, lessons learned, resulting actions and the extent of coverage of the plan were consistently absent.

Agreed Action 4.1

The annual review process will include a section for service managers to complete if they have tested or activated the BC plan in the last year. This should summarise any changes to the plan and the dates of activation or testing. As part of 2021/22 annual review process, plan owners will be asked to include lessons learned from Covid-19.	**Priority** 2 **Responsible Officer** Emergency Planning Manager **Timescale** 31 January 2022

[1] British Standards Institution, *ISO 22301:2012* (2012), p.19, section 8.5.g.

Agreed Action 4.2		
The business continuity policy will be revised to state that service managers and directors are responsible for testing plans in their service areas and directorates periodically. The EPU will conduct strategic business continuity exercises (Council–wide and in conjunction with the Local Resilience Forum). Strategic exercises will be based on national and local (LRF) identified risks.	**Priority**	2
	Responsible Officer	Emergency Planning Manager
	Timescale	31 January 2022

Agreed Action 4.3		
A template will be developed to record the outcomes of exercises, indicating what was tested, conclusions, lessons learned, actions and extent of coverage of the plan in question. Lessons learned from strategic exercises will be shared with business continuity plan owners across the Council.	**Priority**	2
	Responsible Officer	Emergency Planning Manager
	Timescale	31 January 2022

5. Training and feedback

Issue/Control Weakness	Risk
No formal training programme is in place for new or existing plan owners and staff within services. Records of training are not maintained. Introductory sessions to new plan owners are not mandatory.	Training is not provided to officers responsible for maintaining and enacting business continuity plans. This could prevent a prompt and effective response to an event.

Findings

Audit testing found that a formal training programme is not in place for plan owners. EPU staff confirmed they have informal conversations with the officers creating the plans and provide optional introductory sessions to new officers. The introductory training was typically provided during the annual review because that was often when the EPU first became aware of changes in management. As none of this training was documented, it was not possible to assess the quality or consistency of the training provided and whether all plan owners received training during the audit.

The EPU also asks all service managers to provide feedback regarding the quality of the guidance they provide. On some occasions, the EPU will have to ask for targeted feedback to receive any comment. The feedback provided by the EPU during the audit was positive. However, because feedback is only provided when requested it is difficult to know if this sample represents the full extent of officer experience. For these reasons, the EPU only monitors the feedback they receive internally and does not report the results of the feedback outside of the team.

Agreed Action 5.1		
The EPU will develop introduction to business continuity training for consideration by CMT to be part of every managers' induction. The policy review will make clear responsibility for training lies with plan owners beyond this induction. Plan owners will be signposted to the training and awareness materials during annual review process.	**Priority**	2
	Responsible Officer	Emergency Planning Manager
	Timescale	31 January 2022

Agreed Action 5.2		
The business continuity policy will be amended to state that plan owners will provide training to their staff on business continuity and their service's business continuity plan. The annual review process will include a confirmation that the plan owner has made staff aware of business continuity requirements and responsibilities.	**Priority**	2
	Responsible Officer	Plan owners / Emergency Planning Manager
	Timescale	31 January 2022

Audit Opinions and Priorities for Actions

Audit Opinions

Our work is based on using a variety of audit techniques to test the operation of systems. This may include sampling and data analysis of wider populations. It cannot guarantee the elimination of fraud or error. Our opinion relates only to the objectives set out in the audit scope and is based on risks related to those objectives that we identify at the time of the audit.

Our overall audit opinion is based on 4 grades of opinion, as set out below.

Opinion	Assessment of internal control
Substantial Assurance	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 Assurance	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 Assurance	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.

Priorities for Actions

Priority 1	A fundamental system weakness, which presents unacceptable risk to the system objectives and requires urgent attention by management.
Priority 2	A significant system weakness, whose impact or frequency presents risks to the system objectives, which needs to be addressed by management.
Priority 3	The system objectives are not exposed to significant risk, but the issue merits attention by management.

Veritau

Where information resulting from audit work is made public or is provided to a third party by the client or by Veritau then this must be done on the understanding that any third party will rely on the information at its own risk. Veritau will not owe a duty of care or assume any responsibility towards anyone other than the client in relation to the information supplied. Equally, no third party may assert any rights or bring any claims against Veritau in connection with the information. Where information is provided to a named third party, the third party will keep the information confidential.