


GEDLING BOROUGH COUNCIL

INTERNAL AUDIT REPORT

BUSINESS CONTINUITY AND EMERGENCY PLANNING
JUNE 2023

Design Opinion	 Moderate
Design Effectiveness	 Limited

IDEAS | PEOPLE | TRUST



CONTENTS

EXECUTIVE SUMMARY	2
DETAILED FINDINGS	5
APPENDIX I - AFTER INCIDENT REPORT TEMPLATE	14
APPENDIX II - AFTER INCIDENT REPORT TEMPLATE	17
APPENDIX III - LESSONS LEARNT LOG	18
APPENDIX IV - DEFINITIONS	19
APPENDIX V - TERMS OF REFERENCE	20

DISTRIBUTION

Mike Hill	Chief Executive Officer
Alison Ball	Director of Corporate Resources
Francesca Whyley	Head of Governance, Customer Services & Monitoring Officer
Rebecca Hutchinson	Health, Safety and Emergency Planning Manager

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.

REPORT STATUS

Auditors:	Jack Rowan, Auditor Charlotte Thomas, Assistant Manager Gurpreet Dulay, Director
Dates work performed:	6 January - 26 April 2023
Draft report issued:	10 June 2023
Final report issued:	22 June 2023

EXECUTIVE SUMMARY

Design Opinion



Moderate

Design Effectiveness



Limited

Recommendations



SCOPE

BACKGROUND

The Civil Contingencies Act 2004 (the Act) delivers a single framework for civil protection in the UK. The Act establishes a clear set of roles and responsibilities for those involved in emergency preparation and response at a local level. The Act divides local responders into two categories, imposing a different set of duties on each.

Those in Category 1 are organisations at the core of the response to most emergencies (the emergency services, local authorities, NHS bodies). Category 1 responders are subject to the full set of civil protection duties. The Act identifies the Council as a Category 1 responder. As such, are required to:

- Assess the risk of emergencies occurring and use this to inform contingency planning
- Put in place emergency plans
- Put in place business continuity management arrangements
- Put in place arrangements to make information available to the public about civil protection matters and maintain arrangements to warn, inform and advise the public in the event of an emergency
- Share information with other local responders to enhance co-ordination
- Co-operate with other local responders to enhance co-ordination and efficiency.

Gedling Borough Council (the Council) has a service level agreement (SLA) in place with the County council for support with business continuity and emergency planning, however the County Council has been unable to provide the anticipated level of support to the Council due to capacity as the position due to provide the support has not been filled. The previous Health and Safety Officer left the Council in 2021. A new Emergency Planning and Health & Safety Officer started in October 2022. Therefore, while emergency plans and business continuity plans were in place across the Council at the time of review we understand the context that there are due for revision and the health and safety function as a whole is recovering after a period of staffing gaps.

The Council is a member of the Nottinghamshire Local Resilience Forum (LRF).

AREAS REVIEWED

We:

- Reviewed the Council's continuity and emergency framework and relevant policies and procedures
- Performed a detailed review of various Business Impact Assessments (BIAs) and situation preparation/response plans. We sought to

ascertain whether the Council has adequate levels of planning to aid in the creation of a cohesive continuity arrangement.

- Interviews were used to help establish what controls the Council had in relation to the risks that were identified. These reviews were guided by established best practice and the Business Continuity Management Toolkit (BCMT) created by the Government.
- Considerations for IT dependency and training available for appropriate staff were also assessed.
- The interactions between these and the overarching framework also considered.



AREAS OF STRENGTH

During the review, we identified the following areas of strength:

- The Council has emergency and preparation plans in place covering: flooding, sandbags and winter preparation. These are substantial and detailed. They each contain a clear purpose and scope. Roles, points of escalation and contact details are available throughout. We understand the Council is also aiming to produce a hot weather emergency plan, based on the lessons learnt and experiences of 2022
- An emergency plan has also been created for use and in preparation of any situation. The plan provides a good level of detail, makes clear the responsibilities of key personnel and outlines the procedures for escalating and dealing with situations
- Staff training presentations demonstrate management has clear understanding of the requirements of effective business continuity. The presentations provided by the Council and through the Local Resilience Forums (LRF) are concise and provide an opportunity to improve and reinforce understanding of the application of various aspects of business continuity planning
- The Council attended Exercise Lemur and Floodex, as part of the LRF and a tabletop exercise which tested arrangements for national electricity disruption
- The Council has an IT planning procedure through the creation of two detailed documents, the Cyber Incident Response Plan and the DR Protocol, that provide for cyber incidents and loss of equipment
- Incidents are managed through the Council Incident Management Teams (IMTs) then once completed reported up to the Strategic Resilience Group (SRG). We reviewed the minutes to these meetings and noted that there was adequate oversight of incidents and agreed actions. Furthermore, these provided an effective platform for identifying lessons learnt from incidents. For example, following the heatwave in 2022 the IMT and SRG oversaw the Council's response and a Heatwave Response Plan has been developed for future incidents
- The Council is refreshing its corporate business continuity plan and separate plans have been developed by departmental managers for each department. Once approved by the Heads of Service and the Senior Leadership Team (SLT) the Health, Safety and Emergency Planning Manager will work with the departments to test their resilience within certain circumstances. This will support the Council to ensure that the plans, which incorporate business impact assessments, are robust and effective. Heads of Service will be

responsible for ensuring staff are suitably trained and aware of their local business continuity plans.



AREAS OF CONCERN

We identified the following key areas for improvement:

- The Council's BIAs are out of date, of varying quality and the template does not adequately cover business continuity planning, although the Council are currently refreshing these (Finding 1 - High)
- The Business Continuity Policy is out of date and does not have clear links to other policies such as the Emergency Planning Policy Finding 2 - Medium)
- Current BIAs/BCPs and emergency plans are not regularly tested to assess their effectiveness in different emergency situations. The new departmental plans are set to be tested as part of the ongoing refresh process (Finding 3 - Medium)
- Business continuity training attendance is not recorded (Finding 4 - Medium).



ADDED VALUE

Templates for after-incident reporting have been provided along with a lessons learnt log at Appendix I-III.



CONCLUSION

Overall, we have concluded that the Council currently have Moderate controls in place and Limited control design for its business continuity and emergency planning arrangements. However, staff capacity has been improved by the appointment of the Health, Safety and Emergency Planning Manager who has led on a significant exercise to refresh the corporate and service BCPs.

At present plans and procedures are not yet being implemented as envisioned. BIAs are often not treated as live documents by the service managers and in many instances, are out of date.

We also found that there has been infrequent testing of both emergency plans and BIAs to ensure that they are robust There is a risk that the Council is therefore limited in its ability to respond to service disruption and emergency events at present.

While the process the Council are currently undertaking to update the corporate and service BCPs should significantly improve business continuity across the Council, our review was undertaken prior to the completion of this. Therefore, as at April 2023, when our fieldwork was completed the control effectiveness was Limited due to service BCPs being outdated and lacking detail and testing and training not being regularly conducted. However, we would expect that this should improve over the coming months, following the BCPs being updated and tested.

DETAILED FINDINGS

1 BUSINESS IMPACT ASSESSMENTS ARE OUT OF DATE AND DO NOT INCLUDE KEY INFORMATION

TOR Risk:	The Council does not have an appropriate business continuity management framework in place and plans are inadequate. The Council has not identified key aspects of the organisation and the critical systems, activities, and resources on which they depend (taking into account external factors, such as suppliers/services it relies on to perform BAU functions).
Significance:	● High

FINDING

The Council's Business Continuity Policy sets out that each service area should have a Business Continuity Plan (BCP) and that these plans are based on Business Impact Assessments (BIAs). The Government's Business Continuity Management Toolkit (BCMT) indicates that BIAs should be used to identify services and risks associated to them so that further risk assessment and emergency plans can be developed.

In practice however, the Council has a template BIA which is used to document both the BIA and the BCP. The format of the BIA template asks service areas to: identify critical service functions; document the business impact to each function in the event of an adverse incident (including a risk assessment section and an action plan), and provides risk management matrix. It does not place a separate focus on the BCP process.

The Council has BIAs in place for the various service areas, including: Property; Health, Safety and Emergency Planning; Legal; Leisure; Finance and Democratic Services. We established that although all service areas have been covered by the BIAs, due to restructuring, they no longer represent the organisational structure of the Council. The current seven services do not have their own BIAs and instead rely on ones produced for the previous structure.

When we requested BIAs, we found that some service managers were asking for BIAs filled out by previous managers. This indicates that some service managers are unaware of the BIAS for their area. This means they are not regularly updated or easily accessible. Of the six reviewed, five had not been updated since 2020 and the other was last reviewed in 2021. This is not in line with the Business Continuity Policy. However, the Council are currently refreshing its corporate BCP and departmental BCPs which are set to be completed by 30 June 2023. Departmental BCPs will be reviewed by Heads of Service to assess the consistency of quality and that there is no overlap. The Council's target is for these to be approved by the end of July 2023.

Where BIAs were obtained, they were of inconsistent quality, with varying levels of detail. The BIA templates lack fully developed risk management sections. Individual risks are not identified, instead key business interruptions like loss of power or staff are graded. This limits the scope of considerations and does not allow for discussion of specific risks or considerations. In the case of severe risks, there is nothing to indicate whether the risk is being monitored on the corporate risk register.

There is also no opportunity to detail controls that are currently in place to mitigate against risks within the BIA documents. Additionally, some service areas have effectively used the design of the BIA to record impacts that a particular service may have, others however are brief in what they describe and are also brief in what is required to remedy any disruption.

Of the six BIAs assessed, only three provided an adequate level of detail in this area. The Property, Democratic and Finance Service BIAs did not have fully realised impact sections and they all had recovery time objectives (RTO) that did not relate to them. For example, the Finance Service BIA did not identify any impact for disruption to their payroll service for up to a week, yet had an RTO to avoid “irretrievable impacts” of one to four hours. Although critical systems were clearly identified across all BIAs, the risks and requirements they had were not as fully developed.

Actions relating to risks and controls were also underdeveloped across multiple plans. In the Democratic Services BIA, although very high risk had been found, it stated that no actions were identified for electoral registration and the action section was left blank for committee administration. In addition, the Property BIA had 14 actions across all critical functions but only one had a responsible person for implementation. All BIAs had actions that were outstanding, and the Property BIA had eight actions with no comment as to the status of them. How actions were to be measured for success and in what timescale they were to be rolled out is not noted. It could be that the format of the BIA is strengthened by providing a separate section for the action plans (as opposed to an extra column within the risk section), to encourage more consideration to be given. It should also indicate whether the action plan links into any wider Emergency Plans held by the Council and its partners, as well as the formal corporate risk reporting process.

The lack of fully developed BIAs which are regularly updated results in the Council being at risk of not have a solid foundation on which to plan further arrangements. If risks and actions to systems are not being recorded and accessed by necessary personnel, it will be difficult for the Council to gauge whether adequate resources and preparations are in place.



RECOMMENDATION

- a. The Council should ensure that its plan to refresh and implement the corporate and departmental BCPs, incorporating the BIAs, is completed in line with its targeted time scale. It should ensure that the following areas are included within these BCPs:
 - A risk management section should include additional risks and allow for the addition of those identified by service areas. The Community Risk Register held by the Local Resilience Forum, can be utilised to aid this as it details top risks including transport and malicious threats that should be considered
- b. Following the refresh of the BCPs, all service managers should be reminded that they are responsible for maintaining the BIA/BCPs. The Business Impact Analysis for Health, Safety and Emergency Planning, which although is slightly overdue for review, gives a good indication of the level of detail required and how the BIAs can be best utilised. This could be provided as an example of best practice to Service Managers to enable them to improve their own BIA/BCPs
- c. In accordance with the BCP Policy, all BIAs/BCPs should be reviewed periodically or after a significant event to ensure that they are updated in a timely manner. Spot checks on the completion of this should be performed by the Health, Safety and Emergency Planning Manager
- d. The format of the BIA document should be reviewed and amended to include a clearer distinction between the BIA and the BCP. A clear section for a detailed action plan should be included within the document




MANAGEMENT RESPONSE

The corporate BCP and all service BCPs are being refreshed as part of a council-wide exercise, with all service managers given a deadline of 30 June 2023 to have these prepared. These will then be reviewed by Heads of Service to ensure that there is no overlap before approval from SLT. These will incorporate the BIA. Following this, the Business Continuity

Policy will be reviewed/updated. BCPs will be live documents and we will continue to expect service managers to maintain responsibility and ownership of the plans, including ensuring they are kept up-to-date.

Responsible Officer:	Francesca Whyley - Head of Governance, Customer Services & Monitoring Officer Rebecca Hutchinson - Health, Safety & Emergency Planning Manager
Implementation Date:	31 July 2023

2 THE BUSINESS CONTINUITY PLAN DOES NOT IDENTIFY CLEAR LINKS TO THE WIDER BUSINESS CONTINUITY FRAMEWORK

TOR Risk:	The Council does not have an appropriate business continuity management framework in place and plans are inadequate. The Council has not identified key aspects of the organisation and the critical systems, activities, and resources on which they depend (taking into account external factors, such as suppliers/services it relies on to perform BAU functions).
Significance:	 Moderate

FINDING

A Business Continuity Policy should produce the framework for which all other continuity and emergency plans should sit within. It should outline the objectives, required procedures and responsibilities an effective continuity management action should contain. This helps to provide a consistent level of diligence and preparation throughout an organisation to prepare for an event that could impact key systems provided.

The Council's Business Continuity Policy is not well defined. It does not clearly link with other documentation produced and used by the Council, such as the BIAs and the emergency plans. The Business Continuity Plans detailed in the Policy are not used by the Council and are instead merged with BIAs. The Business Continuity Plans, as suggested by the Business Continuity Management Toolkit, are to document a set of procedures that deliver continuity of critical systems. However, these are not fully realised within the BIAs in current usage. Critical functions are also not defined within the policy or in the BIAs. Currently, the BIAs evaluate impacts and risks associated to critical functions but do not go on to determine priorities for recovery of systems or fully outline plans for controls to mitigate against disruption. This disconnect between what the policy sets out and what occurs demonstrates a critical gap in continuity planning.

The policy also makes little mention of other emergency plans the Council has available. For example the GBC Emergency Plan is a detailed and purposeful document but the Business Continuity Policy makes no mention of how it sits within the larger continuity framework. It is unclear how the Emergency Plan is to interact with other plans, BIAs and planning as a whole. Additionally, there is no guidance on how significant risks faced by service areas are to be escalated or added to the Council's corporate risk register where necessary. Following the refresh of the corporate and service BCPs, the Council plan to review and update the Business Continuity Policy.

This means that the Council is at greater risk to confusion and lack of cohesion between different aspects of business continuity planning and the necessary communication between teams. The Council faces the potential risk that key considerations have been overlooked or documents are not utilised in an effective manner.

RECOMMENDATION

The Business Continuity Policy should be updated to reflect:

- a. Current practice with regards to BIAs/BCPs. This should:
 - Identify whether the Council will implement separate BIAs and BCPs or further develop the existing BIAs
 - Establish whether BIAs/BCPs will cover departments or service areas underneath them (where appropriate)

- Give guidance on what critical functions should be considering, including IT, HR, external suppliers and staff/public health & safety
- b. How the Council's Emergency Planning process and plans intersect with BCPs
- c. Outline the process for escalating risks to the Risk Register
- d. The Policy should be reviewed biennially to ensure that it reflects current practice and in particular that roles and responsibilities and any key contact information is up-to-date.




MANAGEMENT RESPONSE

Following the implementation and testing of the new BCPs we intend on reviewing the Business Continuity Policy and Emergency Policy which we recognise are overdue. This should improve the interlinking of the two documents and the overarching Business Continuity Framework. The policies will stand for a few years so will be reviewed every two years.

Responsible Officer:	Francesca Whyley - Head of Governance, Customer Services & Monitoring Officer Rebecca Hutchinson - Health, Safety & Emergency Planning Manager
Implementation Date:	31 December 2023

3 TESTING ON BUSINESS PLANS IS NOT CONDUCTED REGULARLY

TOR Risk:	The plans are not reviewed, kept up to date or exercised therefore no assurance the plans are effective and work as expected
Significance	 Moderate

FINDING

It is expected that both Emergency Plans and Business Continuity Plans are regularly tested, per the Civil Contingencies 2014 guidance.

Testing ensures that arrangements adequately cover the critical systems they are designed for. Regular testing allows for gaps and shared learning to both be considered in further developments. Conducting these exercises also helps to provide training to the staff involved. As discussed by the BCMT, such exercises can help to embed business continuity management across an organisation.

The Council has participated in exercises as part of the Nottinghamshire LRF, and these have provided general feedback to take into consideration for future arrangements. These have provided an opportunity to apply knowledge and processes outlined in plans produced by the Council and the LRF. However, there is not a formal system inside the Council to test the plans that the Council uses nor is there a timetable that establishes when they are to be tested. This means that there is a risk that current plans have not been analysed to identify gaps and outstanding issues.

Additionally, regular testing has not been conducted across all BIA/BCPs. Of the six we have reviewed; we saw no evidence that they had been exercised or updated. Many of the BIAs/BCPs are out of date (see Finding 1) and have not been accessed by service managers, indicating that they have not been adequately exercised in any form. As these are a core element of business continuity arrangements, they too should be regularly exercised to help identify both areas of strength, to help promote good practice, and weakness, to later improve upon. Following the refresh of all BCPs the Health, Safety and Emergency Planning Manager will be undertaking testing of all service BCPs with Heads of Service and service managers. This will include scenario testing the plans to identify any gaps.

RECOMMENDATION

- a. The Council should develop a regular testing schedule/timetable for BCPs and other emergency plans. This should require all BCPs to be tested periodically or after an event. A combination of tabletop, discussion and live exercises should be used, with more frequent checks to ensure contact information, plan activation procedure and plan objectives are up to date and relevant
- b. The Business Continuity Policy should require all service BCPs to be tested biennially, at a minimum, by the Head of Service and service manager, in line with the testing schedule. Heads of Service should be required to confirm that the service plan has been tested to the Health, Safety and Emergency Planning Manager so they can retain a central log for which areas have been tested. Alternatively, due to the Council's small size and limited capacity, it may wish to consider testing the key BCPs, such as finance, ICT, etc more regularly with less frequent testing of other areas. The frequency for each testing in each service area should be agreed and defined in the central log.


MANAGEMENT RESPONSE

There will be detailed testing with each Head of Service and service manager on the BCPs and other emergency plans once they have been refreshed. This will involve scenario testing

to assess how the service BCPs stand up to different scenarios, ie loss of electricity and power in the Council offices. A log can be maintained thereafter and monitored by the Health, Safety and Emergency Planning Manager for annual/periodic testing of BCPs with the confirmation from Heads of Service.

Responsible Officer:	Francesca Whyley - Head of Governance, Customer Services & Monitoring Officer Rebecca Hutchinson - Health, Safety & Emergency Planning Manager
Implementation Date:	31 December 2023

4 TRAINING LOGS HAVE NOT BEEN RETAINED FOR STAFF THAT HAVE ATTENDED SESSIONS

TOR Risk:	Training is not undertaken by those involved in implementing the plan
Significance	 Low

FINDING

Training ensures staff are adequately prepared and familiar with their duties and the procedures that they are to carry out and follow. For business continuity, familiarisation with details of critical systems and the requirements to keep them running are areas that thorough training can support in implementation and support of arrangements.

The Council has taken participated in several events that have been run through the Nottinghamshire LRF to exercise situations and ensure staff understand their roles and the details of responses to events. As part of the process for updating BCPs, the Council held a workshop with service managers to train them on what information needs to be included in their service BCPs, specific incident training on how to respond to an emergency and guidance on training staff on the BCPs. A training log of attendance was maintained for this session and Heads of Service have requested a further session for managers that were unable to attend.

However, while staff will be trained within their department on the new service BCPs once they have been agreed, training logs are not currently kept to record which staff have been trained out on the plans. Training logs would enable the Council to identify further training requirements and thus prioritise specialist training for members of staff who require it. This means the Council is currently at risk to staff being inadequately prepared to situations as although training may have been available, it may not have been attended. Similarly, a training log is in place to record what training the SLT, Heads of Service and managers have completed, including BCP and emergency planning, but the nature of the training completed is not stated.

We were informed that Heads of Service will be responsible for training staff within their service on the contents of the new service BCPs once they have been refreshed and tested.

RECOMMENDATION

- Heads of Service should establish a training log to record the attendance of members of staff for any training provided on the new service BCPs
- The training log for SLT, Heads of Service and managers should be clearer on the nature of the training provided on BCP and emergency planning.

MANAGEMENT RESPONSE

Training has been provided to service managers in preparation for the updating of all service BCPs to ensure that they are aware of what should be included, and also specifically on incident responses. A training log can be recorded for future similar training. Heads of Service will be responsible for ensuring that all staff in their service are aware of the updated service BCPs and understand the processes they need to follow in the event of an emergency.

Responsible Officer:	Francesca Whyley - Head of Governance, Customer Services & Monitoring Officer
-----------------------------	---

Implementation Date:

Rebecca Hutchinson - Health, Safety & Emergency Planning
Manager

31 December 2023

APPENDIX I - AFTER INCIDENT REPORT TEMPLATE

After Incident Report

Conducted on:

At/Via:

Incident Name:

Incident Reference:

Individuals involved in the Meeting were:

Role	Role Holder	Role	Role Holder

Additional Attendees (if required):

Name	Role	Name	Role
Incident detection and escalation:			

Command:
Information available:
Communications:
Effectiveness of the plan:
Decisions made:
Response of staff:
Costs and expenses:
Training implications:
Impact on *Organisation* :

Other comments:

APPENDIX II - AFTER INCIDENT REPORT TEMPLATE

After Incident Report			
Incident Name:			After Incident Report Date:
Incident Reference:			
Names of Participants:			
Objectives & Success Factors:			
Timeline of events:		Details of Events:	
Areas of Strength:			
Areas of Improvement:			
Key Takeaways:			
Recommendation	Actions	Due Date	Responsible Party

APPENDIX III - LESSONS LEARNT LOG

Lessons Learned Log								
TITLE					Manager:			
Date Logged	Incident Reference	Incident Date	Event	Recommendation	Action	Due Date	Responsible Party	Follow Up
date added to log	*incident reference from report*	*date of incident*	*brief details on event*	*details of change to be implemented*	*specifics on how changes will be implemented*	*when they will be implemented by*	*who is/are responsible for the implementation*	*how will the changes be assessed*

APPENDIX IV - 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.

APPENDIX V - TERMS OF REFERENCE



KEY RISKS

Based upon the risk assessment undertaken during the development of the internal audit operational plan, through discussions with management, and our collective audit knowledge and understanding the key risks associated with the area under review are:

- The Council does not have an appropriate business continuity management framework in place and plans are inadequate. The Council has not identified key aspects of the organisation and the critical systems, activities, and resources on which they depend (taking into account external factors, such as suppliers/services it relies on to perform BAU functions)
- Planned dependency on IT functionality is not sufficiently coordinated between Business Continuity and Emergency Planning activities
- Significant risks threatening the performance of critical functions in the event of an emergency or disruption are not identified, meaning resources are not focussed in the right areas
- Training is not undertaken by those involved in implementing the plan
- The plans are not reviewed, kept up to date or exercised therefore no assurance the plans are effective and work as expected
- Post incident reporting is ineffective therefore not allowing appropriate lessons to be learned and/or shared. Actions for improvement are not followed up.



SCOPE & APPROACH

The following areas will be covered as part of this review:

- **Business Continuity/ Emergency Plans** - we will review these are in place, communicated to staff and published (where there is a positive benefit in doing so). We will review whether these appropriately interact with local service plans and identify key aspects of the organisation and the critical systems, activities and resources on which they depend. We will also review whether they can be easily understood and are not unnecessarily complex
- **Risk assessments** - We will review what risks have been assessed that could potentially threaten the Council's critical functions, and how the Council's risk registers link to the business continuity/emergency plans in place
- **External factors** - We will review how the Council has ensured that organisations delivering services on their behalf or capabilities which underpin service provision can deliver to the extent required in an emergency
- **Training** - It is important that relevant people across the Council are confident and competent in enacting the plan. We will review the training timetable in place (ensuring training takes place before the plan is exercised) and who has received training. We will also review the content of the training ensuring it covers:
 - The contents of the plan - how is the plan invoked? What are the key decision-making processes? Who else needs to be involved?
 - Their role in implementing the plan - what is expected of them? How do they fit into the wider picture?
 - Key skills and knowledge required in crisis response.
- **Exercising** - Under the Act plans cannot be considered reliable until they have been exercised and proved to be workable. We will review the exercising timetable in place and assess whether timescales are appropriate and whether all parts of the plan are covered. We will assess the last two exercises undertaken and ascertain whether the exercise:
 - Validated the plans to ensure they work

- Rehearsed key staff ensuring they were familiarised with what is expected of them in a crisis and preparing them for crisis conditions
- Tested the systems that the Council rely upon to deliver resilience (eg uninterrupted power supply) function correctly and offer the degree of protection expected.
- **Reviewing** - the Act requires category 1 responders to maintain their business continuity plans. We will ascertain:
 - How frequently the plans are reviewed
 - Who is involved in the review
 - Whether they are updated as per an incident or exercise, or changes in key personnel, suppliers or contractors
 - If plans are updated as per changes to risk assessments or business objectives.
- **Lessons Learnt** - ensure there are lessons learnt reports in place after the plan has been exercised. Review the lessons learnt and resulting action plans, ascertain if actions have been assigned an owner, have been implemented as per the agreed timescales and action taken where dates have been missed.

However, Internal Audit will bring to the attention of management any points relating to other areas that come to their attention during the course of the audit. We assume for the purposes of estimating the number of days of audit work that there is one control environment, and that we will be providing assurance over controls in this environment. If this is not the case, our estimate of audit days may not be accurate.

FOR MORE INFORMATION:

Gurpreet Dulay

Gurpreet.Dulay@bdo.co.uk

The matters raised in this report are only those which came to our attention during the course of 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.

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.

Copyright ©2023 BDO LLP. All rights reserved.