

| | |
|-------------------|--|
| Report of: | Director of Legal and Governance Services (Monitoring Officer) |
|-------------------|--|

| | |
|----------------------|-----------------|
| Submitted to: | Audit Committee |
|----------------------|-----------------|

| | |
|--------------|-----------------|
| Date: | 6 February 2025 |
|--------------|-----------------|

| | |
|---------------|--|
| Title: | Business Continuity Annual Assurance Report 2024 |
|---------------|--|

| | |
|--------------------|-------------|
| Report for: | Information |
|--------------------|-------------|

| | |
|----------------|--------|
| Status: | Public |
|----------------|--------|

| | |
|-----------------------------------|-----------------------|
| Council Plan priority: | Delivering Best Value |
|-----------------------------------|-----------------------|

| |
|--------------------------|
| Executive summary |
|--------------------------|

| |
|--|
| This report sets out the arrangements in place to ensure the Council meets its legal obligations in relation to Business Continuity. The report sets out the Business Continuity governance framework, actions delivered during 2024 and planned actions for 2025. |
|--|

Purpose

1. The purpose of this report is to outline the Council's approach to business continuity management, summarise activity in the past year and planned activity for 2025, to provide the Committee with assurance that the Council has robust arrangements in place, as required by the Civil Contingencies Act 2004.

Recommendations

2. That the Committee considered whether it has been provided with sufficient information to be assured that the arrangements in place to manage business continuity within the Council are sufficient to ensure compliance with legal requirements and the Local Code of Corporate Governance.

Rationale for the recommended decision(s)

3. To support the Committee to discharge its responsibility to maintain an overview of arrangements in place to ensure good governance.

Background and relevant information

4. The Council has a duty under the Civil Contingencies Act 2004 to develop and maintain business continuity plans to enable continued delivery of 'business critical functions' during a 'business interruption' event.
5. Business continuity planning is separate to emergency planning, which sets out how the Council responds to emergency incidents that impact on residents and businesses, though there will be times where the two disciplines interrelate.

The Council's approach

6. The Council's Corporate Business Continuity Plan defines critical functions as those which, if interrupted could result in:
 - risk of serious injury;
 - risk of death;
 - massive financial losses; or
 - significant damage to the Council's reputation.
7. The Council will consider activating its business continuity plans if there is a business interruption event that:
 - is likely to last for more than half a working day;
 - affects a vulnerable group of service users;
 - impacts on the delivery of key critical activities;
 - restricts access to one of the key council buildings;
 - could generate significant damage to the Council's reputation; or
 - is highly likely to escalate into one of the above categories.
8. The Council has the following plans in place to respond to the variety of events that could occur:

- the Corporate Business Continuity plan;
 - supporting Departmental Business Continuity plans;
 - Relocation Plan;
 - ICT Disaster Recovery Plan.
 - Fuel Plan;
 - Pandemic Plan.
9. The Council does not publish its business continuity plans as they outline sensitive information around its critical functions and their recovery that could be misused and contain personal information relating to employees that have agreed to share personal contact details to enable the Council to get in touch with them quickly in the event of an incident. Therefore, the paragraphs below outline the content of the Council's plans only in broad terms.
10. The **Corporate Business Continuity Plan** is the overarching plan for the organisation. It sets out the structure used to identify and prioritise critical functions; mechanisms for enacting the plan; how all plans are maintained, tested and reviewed; and policies and procedures in place to support effective business continuity planning.
11. Supporting **Departmental Business Continuity Plans** set out detailed recovery arrangements for each critical function or activity, by Directorate of the Council, outlining information on buildings used to deliver the function or activity, staff information, key equipment and supplies, key records, ICT systems and other key contacts.
12. The **Relocation Plan** sets out how critical functions / activity would be relocated to other buildings within the Council's estate or employees sent home to work using agile working solutions, if one or more buildings became inaccessible.
13. The Council's approach is, in the main, not to write numerous plans for risks to critical functions. The ICT Disaster Recovery Plan, Fuel Plan and Pandemic Plan are exceptions to this rule, created in response to specific risks that have faced local authorities and the scale of the interruption that such events have and could cause.
14. The **ICT Disaster Recovery** Plan focuses on maintaining ICT for business critical functions, highlighting those applications which are hosted externally, and any services supported by the Council's key partners.
15. The **Fuel Plan** outlines how the Council would respond to a fuel shortage to ensure business critical staff are able to continue to do their work.
16. The **Pandemic Plan** was created in 2022 by merging two previously separate plans in relation to flu and Covid-19. The refresh reflected learning from COVID-19 pandemic and previous pandemics including but not limited to influenza and SARS.
17. During 2024, the Council also put in place a Business Continuity Policy, which articulates the Council's approach to Business Continuity. This was formally agreed by the Mayor in December 2024.

Plan testing

18. The Council aims to test its plans at least once every 12 months, or produces a lessons learned report if a live incident has occurred during the past year. During 2024/5 the

Local Government Association (LGA) facilitated an Incident Response (IR) Exercise for Middlesbrough Council. This exercise focuses specifically on challenging the IT team's response to a cyber incident, offering an opportunity to review their plans, rehearse individuals, and to learn how, and whether it could be improved. Recognising the growing cyber threat facing all institutions, including local government, Middlesbrough Council requested LGA support them in defining and conducting a suitably challenging incident response exercise for the IT team, using a plausible threat scenario, to validate response capabilities and enhance processes, procedures and documentation.

Review schedule

19. In a normal planning cycle, business continuity plans are updated every six months, and reviewed on an annual basis (May and November) with the scale of the review dependent on the level of organisational change that has occurred in the intervening period. In some years this means that only minor updates (e.g. contact details) are required, in others fundamental reviews will be required to reflect changes to the Council's structure or other significant developments e.g. where services have been outsourced, or brought back in house.
20. During the 2024/5 annual review of plans, there was an increased focus on the impact of the loss of ICT and how it could have an impact on critical activities to ensure services planned effectively for this event.

Activity in 2023/4

21. The following actions were delivered during 2024/5 to ensure good governance in relation to business continuity.

Testing

22. Generator failover tests were carried out at both of the Council's data centres during the summer and winter of 2024 which involved testing the resilience of the generators, Uninterrupted Power Supply (UPS) systems and also environmental (e.g. fire suppression) systems. This test ensured that in the event of a major power outage within the town or the loss of one of the data centres entirely, the other data centre will continue to support the Council's business critical applications, with no changes required.
23. LGA facilitated an Incident Response (IR) Exercise for Middlesbrough Council ICT to validate response capabilities and enhance processes, procedures and documentation.
24. In November 2024, Middlesbrough Council were subject to several distributed denial-of-service (DDoS) attacks. This is a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.

Documentation

25. All Corporate Business Continuity Plans were updated in November 2024, refreshing the content, updating the formatting, contacts and aligning processes with best practice.

26. An update and full review of Directorate Business Continuity plans has been undertaken within the year to reflect changes in the service, location, employee details and to reflect the additional measures that would be required to ensure resilience to any loss of electricity and ICT services.
27. An offsite location has been developed to hold all business continuity plans and critical function plans to further strengthen access to plans should an business continuity event occur.

Communication

28. To further strengthen Middlesbrough Council's Business Continuity processes, a detailed Business Continuity Policy has been written (as set out in the plans and policies section) and approved by Single Executive in December 2024. The policy will:
 - Set out how the Council will to anticipate risks, mitigate where possible to reduce the likelihood of its services being interrupted.
 - The plans it will put in place to manage service interruptions; and
 - The maintenance and testing of those plans to ensure they remain fit for purpose.

Business Continuity activities for 2025/26

29. During 2024/25, further work will be undertaken to build on progress made in 2024/25 part of the Council's commitment to continual improvement in business continuity planning.

Training

- Officers plan to undertake a combined EMRT and BC exercise to test the effectiveness of the relocation plan.
- Further develop critical function plans and test on a key system to ensure that the ICT Disaster Recovery Plan is exercised to test its effectiveness.
- Deliver training for senior officers pertaining to decision making, media and communications and roles and responsibilities.

Documentation

- Undertake the annual full review and update of all business continuity plans to ensure they remain fit for purpose.
- Battleboxes to be updated by business-critical services to enable service delivery to be maintained in the event of a cyber-attack or power cut with a focus on locations of battleboxes.
- Revision of plans to reflect occupation of new structures and offices this year.
- Improve processes within the Corporate Business Continuity room in Fountain Court and refresh plans for the relocation site to ensure both are fully equipped to respond to a business interruption and provide quick response guides and terms of reference for all Business Continuity Leads.

Communication

- Communications Plan for Business Continuity to be enhanced to cover communications in the absence of ICT system.
- Delivery of a hierarchical priority system requirement for ICT to be signed off by the Head of Paid Service.

Rationale for the recommended decision

30. To support the Committee to discharge its responsibility to maintain an overview of corporate governance within the Council, which includes business continuity management.

Other potential decisions and why these have not been recommended

31. Not applicable.

32. Impact(s) of the recommended decision(s)

| Topic | Impact |
|--|--|
| Financial (including procurement and Social Value) | There are no new direct financial considerations in relation to business continuity management as a result of this report. By having robust plans in place, the Council will be better placed to mitigate financial impacts from any interruption event. |
| Legal | Business continuity is a part of corporate governance, and the Council has a legal duty to ensure arrangements comply with the requirements of the Civil Contingencies Act 2004. |
| Risk | <p>Business Continuity impacts positively on the following risks managed within the Legal and Governance Services Directorate Risk Register:</p> <ul style="list-style-type: none"> • O8-037 - If business continuity plans are not fit for purpose then in the event a business interruption the Council would potentially be unable to provide critical services which could result in harm to service users and a breach of law namely the Civil Contingencies Act 2004. • O8-052 - Risk of disruption to service delivery, Due to: Lack of adequately tested Business Continuity / Disaster Recovery Plans which fail to effectively manage a critical incident (e.g. relating to access to critical systems / data) and further extend the period of system unavailability. Resulting In: extended or permanent loss of systems/data, poor communication and the inability to identify and inform key officers about incident /implications. Failure to reinstate services/systems within an appropriate timescale, dissatisfaction/loss of confidence with the |

| | |
|---|--|
| | Council's customers. |
| Human Rights, Public Sector Equality Duty and Community Cohesion | There are no direct implications from this report on human rights, equality and diversity. |
| Climate Change / Environmental | Not applicable. |
| Children and Young People Cared for by the Authority and Care Leavers | Good business continuity management and Disaster Recovery within Children's Services and Adult Social Care and Health Integration directorates will ensure that the correct level of support is given during a business continuity event to Children, Young People and Care Leavers. |
| Data Protection | Business Continuity and Disaster Recovery arrangements are a critical control in order to ensure compliance with data protection legislation in particular the availability of personal data to avoid personal data breaches. |

Actions to be taken to implement the decision(s)

| Action | Responsible Officer | Deadline |
|--|---------------------|------------|
| Implement the actions laid out in the plan for 2025/26 | Gary Welch | 31/03/2026 |

Appendices

None.

Background papers

| Body | Report title | Date |
|---------------------------------------|---|------------------|
| Audit Committee | Business Continuity – Annual Assurance Report | 30 June 2024 |
| Audit Committee | Business Continuity – Annual Assurance Report | 31 March 2023 |
| Corporate Affairs and Audit Committee | Business Continuity – Annual Assurance Report | 31 March 2022 |
| Corporate Affairs and Audit Committee | Business Continuity – Annual Assurance Report | 4 February 2021 |
| Corporate Affairs and Audit Committee | Business Continuity – Annual Assurance Report | 19 December 2019 |
| Corporate Affairs and Audit Committee | Business Continuity – Annual Assurance Report | 6 December 2018 |

Contact: Gary Welch, Strategic Risk and Health and Safety Manager
Email: gary_welch@middlesbrough.gov.uk