MIDDLESBROUGH COUNCIL

Report of:	Chief Executive
Submitted to:	Audit Committee
Date:	19 February 2026
Title:	Business Continuity Annual Assurance Report 2025
Report for:	Decision
Status:	Public
Council Plan priority:	Delivering Best Value

Proposed decision(s)
That the Audit Committee: **NOTES** the arrangements in place to manage Business Continuity within the Council and progress within the last year. **CONSIDERS** whether the information provided has given the Committee sufficient assurance that the Council has appropriate arrangements in place in relation to Business Continuity.

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 2025 and planned actions for 2026.

1. Purpose

1.1 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 2026, to provide the Committee with assurance that the Council has robust arrangements in place, as required by the Civil Contingencies Act 2004.

2. Recommendations

2.1 That the Audit Committee:

- **NOTES** the arrangements in place to manage Business Continuity within the Council and progress within the last year.
- **CONSIDERS** whether the information provided has given the Committee sufficient assurance that the Council has appropriate arrangements in place in relation to Business Continuity.

3. Background and relevant information

3.1 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.

3.2 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

3.3 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.

3.4 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.

3.5 The Council has the following plans in place to respond to the variety of events that could occur:

- Corporate Business Continuity plan;

- supporting Departmental Business Continuity plans;
- Relocation Plan;
- ICT Disaster Recovery Plan;
- Fuel Plan; and
- Pandemic Plan.

3.6 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.

3.7 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.

3.8 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.

3.9 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.

3.10 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.

3.11 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.

3.12 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.

3.13 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.

3.14 The Council also has a Business Continuity Policy, which articulates the Council's approach to Business Continuity.

Plan testing

3.15 The Council aims to test its plans at least annually or, where a live incident has occurred within the past year, produce a lessons-learned report. During 2025/26, the Council experienced several live incidents, including a Distributed Denial of Service (DDoS) attack targeting our ICT security systems. Thanks to planning undertaken in the

previous year, the Incident Response (IR) process proved effective. Additionally, the Council implemented its relocation plan for Middlesbrough House staff following a flooding event.

Review schedule

3.16 Under a normal planning cycle, business continuity plans are updated every six months and undergo a formal review annually (in May and November). The scope of each review depends on the extent of organisational change during the intervening period. In some years, only minor updates—such as contact details—are necessary, while in others, comprehensive reviews are required to reflect significant changes, such as restructuring or major service delivery adjustments (e.g., services being outsourced or brought back in-house).

3.17 During the 2025/26 annual review of plans, particular emphasis was placed on assessing the potential impact of ICT system loss and its effect on critical activities. This focus ensured that services were adequately prepared and planned to manage such an event effectively.

Activity in 2025/6

3.18 The following actions were delivered during 2025/6 to ensure good governance in relation to business continuity.

Training

- Officers successfully undertook a joint EMRT (Emergency Management Response Team) and Business Continuity exercise to test the effectiveness of the relocation plan.
- Further developed critical function plans and tested a key system to ensure the ICT Disaster Recovery Plan was exercised and validated for effectiveness.
- Delivered training for senior officers focused on decision-making, media and communications, and roles and responsibilities during incidents.

Documentation

- Undertook a full annual review and update of all Business Continuity Plans to ensure they remain fit for purpose.
- Updated battle boxes for business-critical services to maintain service delivery during a cyber-attack or power outage, with a focus on their locations.
- Revised plans to reflect new staffing structures and offices introduced this year.
- Improved processes within the Corporate Business Continuity Room at Fountain Court and refreshed relocation site plans to ensure both are fully equipped to respond to business interruptions. Provided quick response guides and Terms of Reference for all Business Continuity Leads.

Testing

- Conducted failover tests at Council data centres during summer and winter 2025. These tests validated the resilience of generators, Uninterrupted Power Supply (UPS) systems, and environmental systems (e.g., fire suppression). The results confirmed that in the event of a major town-wide power outage or complete loss of a data centre, the Council will continue to be able to operate.

- Completed fibre testing on all essential loops to ensure line integrity. This process will be repeated bi-annually to proactively identify and prevent potential weaknesses.
- In September and October 2025, a tabletop exercise was conducted across all directorates, ensuring participation from key personnel, including directors and heads of service. The exercise focused on Critical Function Plans and how these would operate during a cyberattack or service relocation scenario. The objectives were to:
    - Raise awareness of Critical Function Plans.
    - Refresh knowledge of each directorate's Business Continuity Plan.
    - Identify areas for improvement within the plans.
    - Familiarise staff with the heightened risk of a cyber outage and its potential impact on service delivery.
    - Prepare staff for the implications of relocating staff and services.
    - Develop actions based on lessons identified to address any gaps in the plans.
- A detailed "Lessons Identified" report was shared with all directorates, and these insights were incorporated into the Business Continuity Improvement Plan.
- As part of the North East local authorities' collaborative efforts, Middlesbrough Council participated in a regional exercise designed to test Public Health responses to a pandemic scenario. The exercise commenced in September 2025 and concluded in November 2025. Middlesbrough Council's Pandemic Business Continuity Plan was acknowledged as an example of best practice, and a redacted version was shared with the partners.

Documentation

- All Corporate Business Continuity Plans were updated in November 2025, refreshing the content, updating the formatting, contacts and aligning processes with best practice.
- 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.
- An offsite location has been developed to hold all business continuity plans and critical function plans to further strengthen access to plans should a business continuity event occur.

Business Continuity activities for 2026/27

3.19 During 2026/27, further work will be undertaken to build on progress made in 2025/26 as part of the Council's commitment to continual improvement in business continuity planning.

Training

- Plan and conduct a joint EMRT (Emergency Management Response Team) and Business Continuity exercise to test the effectiveness of the relocation plan.
- Further develop critical function plans and perform a test on a key system to ensure the ICT Disaster Recovery Plan is exercised and validated for effectiveness.
- Conduct a tabletop exercise in collaboration with the North East Regional Cyber Crime Unit (NERCCU) to test ICT protocols and engage business leads in evaluating response effectiveness.

- Deliver targeted training for senior officers on media and communications, as well as their roles and responsibilities during incidents.
- Ensure key officers attend a Capability Evaluation and Exercising course to align with best practice standards.
- Facilitate attendance and completion of ISO 22301 training for key officers, providing a framework for a robust Business Continuity Management System.
- Provide directorates with training on MBC policies regarding data protection and Bring Your Own Device (BYOD) to ensure compliance with current legislation and Council policy.

Documentation

- Undertake a comprehensive annual review and update of all Business Continuity Plans to ensure they remain fit for purpose and aligned with current organisational needs.
- Update plans to reflect the occupation of new structures and offices introduced this year.
- Enhance processes within the Corporate Business Continuity Room at Fountain Court and refresh relocation site plans to ensure both are fully equipped to respond effectively to business interruptions. Provide quick response guides and clear Terms of Reference for all Business Continuity Leads.
- Renew and update roles and responsibilities cards where necessary to maintain clarity and accountability.
- Test Environment Community and Culture relocation plans to confirm robustness, particularly in line with the implementation of newly purchased equipment.
- Conduct Business Impact Analysis (BIAs) across all directorates to review software interdependencies, ensuring accurate mapping and identification of interlinks between systems.

Communication

- Heads of Service to review and collaborate with team members to provide up-to-date contact details to ensure they can be reached promptly in the event of a Business Continuity incident.
- Data Cuts for Resilience, Directorates should explore and implement data cuts, with associated secure storage and refresh plans, where critical data is required for the effective operation of service areas. This will enhance resilience during an ICT outage by enabling rapid restoration and access to essential data.

4. Other potential alternative(s) and why these have not been recommended

4.1 Members could choose to decide that they do not have sufficient information to be assured that the Council's governance in relation to Business Continuity is sufficient.

4.2 This is not recommended as sufficient information has been provided.

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

Topic	Impact
Financial (including procurement and Social Value)	There are no new direct financial implications arising from this report in relation to business continuity management. However, by maintaining robust continuity plans, the Council is better positioned to mitigate potential financial impacts resulting from service interruptions, ensuring cost efficiency and protecting social value commitments.
Legal	Business continuity is a fundamental component of corporate governance, and the Council has a statutory duty to ensure its arrangements comply with the Civil Contingencies Act 2004. These requirements help maintain resilience and preparedness in the face of emergencies, safeguarding essential services and public confidence.
Risk	Business Continuity impacts positively on the following risks managed within the Legal and Governance Services Directorate Risk Register: • 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.
Reducing poverty	Effective business continuity management and disaster recovery within the Local Authority are essential to maintaining critical services that support individuals in poverty. By ensuring these services remain operational and can resume normal activities quickly and efficiently during an incident, we help minimise disruption and safeguard vulnerable communities.
Climate Change/ Environmental	Not applicable.
Children and Young People Cared for by the Authority and Care Leavers	Effective business continuity management and disaster recovery within the Children's Services and Adult Social Care and Health Integration directorates are vital to ensuring that the appropriate level of support is maintained during a

	business continuity event. This approach safeguards the wellbeing of Children, Young People, and Care Leavers by minimising disruption and enabling essential services to continue without delay.
Data Protection	Robust business continuity and disaster recovery arrangements are essential controls for ensuring compliance with data protection legislation. In particular, these measures help maintain the availability of personal data during disruptions, reducing the risk of personal data breaches and safeguarding sensitive information.

Background papers

Body	Report title	Date
Audit Committee	Business Continuity – Annual Assurance Report	06 February 2025
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

Contact: Gary Welch, Strategic Risk and Health and Safety Manager

Email: gary_welch@middlesbrough.gov.uk