Critical Service Business Continuity (BC)
BC planning including ICT risk

BC Internal Audit and plan review what we are doing

Leicestershire County Council

Ongoing Business continuity management work (critical Service Plans includes:

- An in-depth capability assessment of each tier one operational BC plan will be carried out. (There are approximately 42 Tier 1 critical plans including Department Management Team (DMT) plans)
- Creation of an ongoing procedure to confirm levels of assurance after initial review program has completed
- Assist teams in completing and improving content held with in BC plans, providing bespoke guidance where needed to each team
- Providing relevant BC Training where required

BC plan I/A and review expected outcomes

Leicestershire County Council

Governance and review:

- Quarterly reports are generated for Resilience Planning Group (RPG) on the progress of the reviews, current levels of assurance, and any issues or opportunities discovered
- An increased level of assurance is expected after this process. Two factor assurance (ISO Compliance – Testing and validating)
- A process for reviewing & assessing BC plans including testing
- Raised awareness around BC plans and the part they play during an incident
- Annual report to Corporate Governance Committee

Business Continuity V Disaster Recovery

Leicestershire County Council

KEY DIFFERENCES BETWEEN BUSINESS CONTINUITY VS DISASTER RECOVERY

C2	Business Continuity	Disaster Recovery
Objective	To maintain operation during and after a disaster, ensuring critical functions remain available.	To restore data access and IT infrastructure after a disruption.
Scope	Broader, including IT, manufacturing, customer service, and supply chain management.	Narrower, focusing specifically on IT systems, data recovery, and technical aspects.
Planning & Strategy	Involves strategies for operational challenges, alternative work locations, manual workarounds, and communication.	More technical, detailing data backups, system recovery, server restoration, and emergency power supply.
Timeframe	Proactive and long-term, ensuring continuous operations during and immediately after a disruption.	Reactive, focusing on immediate IT recovery post-disaster with specific RTOs and RPOs.
Testing & Maintenance	Testing involves simulating disaster scenarios to ensure continuity and employee readiness.	Testing involves restoring from backups, checking IT infrastructure integrity, and recovery procedures.

BC planning and IT issues

- BC plans (consequence management) contain a section on contingency arrangements (section 6 of the BC plan template)
- As part of this the following areas relating to IT are:
  - » Loss of IT systems
  - » Loss of telephony
  - » Loss of critical information (including – data)
- In this section Teams should detail their options for the loss of any of the above
- The decision on how this is achieved is down to individual teams and DMT's as this is linked to their delivery of critical services (with support from BC officers if required)
- As part of the reviewing process teams are encouraged to get advice from relevant departments/teams, particularly around IT issues whether that be an internal or external provider plan

IT outage issues

- In the event of an IT incident, the team(s) affected should follow the Council's Incident Management Plan (IMP) and inform the On Call Senior Manager (OCSM)
- Once the OCSM is notified of an incident RPG (dependent on severity) maybe set up to initially oversee actions.
- If RPG is set up the Resilience and Business Continuity (R&BC) team will then support RPG
- In the event of a large scale even total LCC IT incident both RPG and the Corporate Management Group would need to meet (in person)
- If the incident affects more LRF partners, the R&BC team will also support the broader Resilience Partnership