Overview of BC/DR test preparation

V1.1

LOCAL DIGITAL Cyber

Objective

Outline guidance and approach to enable preparation to perform Business Continuity DR Testing of Local Authority (LA) Council information systems.

This follows on from the BIA definition of the service criticality and the RPO & RTO definition. The agreed RTO/RPO drives the backup design and infrastructure solution, which is then tested as part of a BC/DR exercise at least annually to ensure you can recover in the event of a disaster.

BC/DR testing will enable Local Authorities to prove their ability to recover following a ransomware attack or a disaster.

LOCAL
DIGITAL | Cyber

CTP connections

Mission Critical service resilience and recovery.
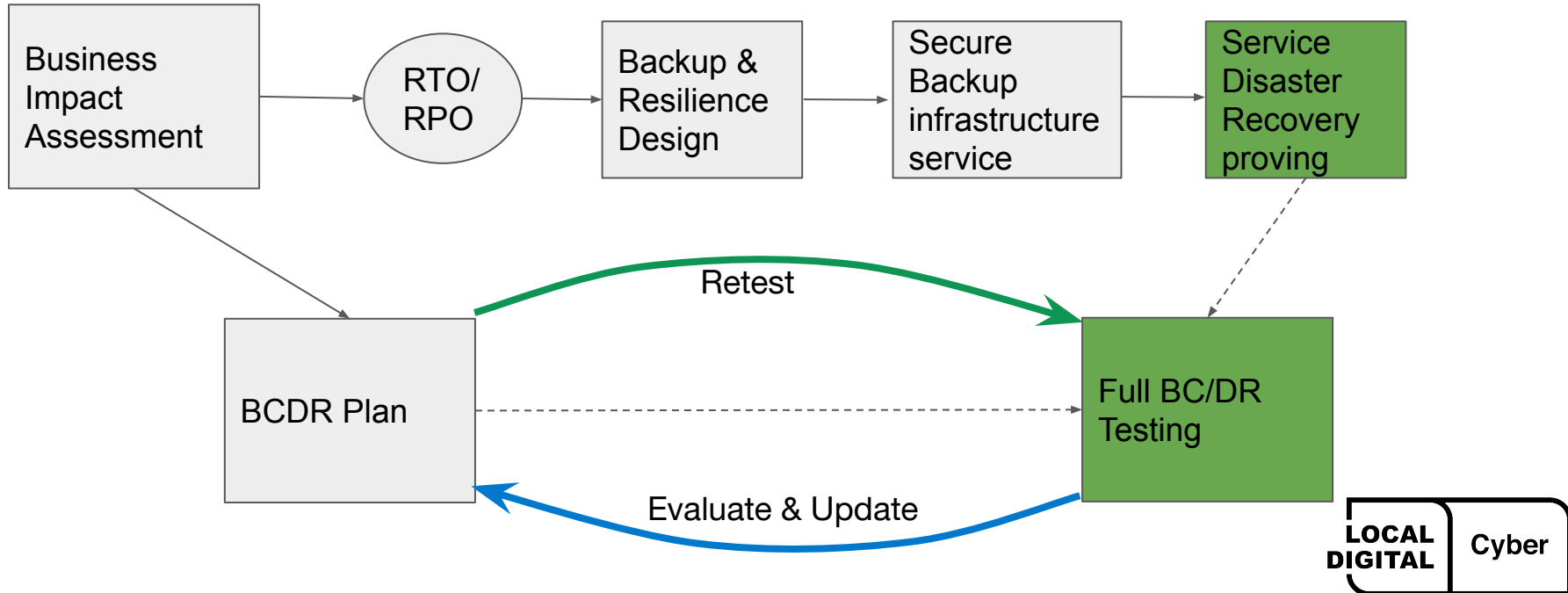
BC/DR definition

Business Continuity and Disaster Recovery (BC/DR) is a set of processes and techniques used to help an organisation recover from a major incident/disaster and continue or resume routine business operations. It is a broad term that combines the roles and functions of IT and business in the aftermath of a disaster.

The Local Authorities Business Continuity Plan should to cover all elements of the end to end business in case of an incident.

An incident management plan is a key element to ensuring effective recovery from an incident.

For cyber security incidents which impact IT services the NCSC has guidelines here which advise on the 10 steps to Cyber Security.

LOCAL DIGITAL | Cyber

BC/DR plan definition

Devise a consistent plan, and ensure all plan components are fully accessible in the event of a major disaster

- Make sure the BC/DR plan will work with or without the internal key people who developed it

- Make sure your BC/DR plan is accessible offsite and with no access to internal IT Systems

- Prioritise Applications Recovery Order and the dependencies each have

- Create your plan with the mentality that anything can happen.

- Detail the high level approach, identifying the core infrastructure services required to run a service in DR (gold builds, backups, batch schedulers, network data flows, DNS, compute power, storage etc)

LOCAL DIGITAL | Cyber

Why is BC/DR testing important?

It tests the LA's ability to respond to incidents that could affect the operation of essential functions/services.

The test exercises should reflect past experience, scenario planning, or threat intelligence and should draw heavily on risk assessment, considering all relevant assets and vulnerabilities, especially where they relate to essential services.

It also enables the Local Authority to understand the complexity of the IT Recovery process in terms of:

- The Data Centre services that are prerequisites to a recovery, e.g. networks, storage, DNS, Active Directory, desktop services etc;

- The personnel and skills required to be available to perform recovery;

- Proving that the the recovery is possible within target RPO & RTO.

LOCAL DIGITAL | Cyber

How to perform a BC/DR test

- Test the plan: An initial "dry run" of the plan is performed by conducting a structured walk-through test. An actual test-run must then be performed and any problems encountered are corrected.

- This cycle of Test, Evaluate and Update (the BCDR Plan) is a key activity to ensure the plan is current, achievable and practicable.

- Take a staged approach:
  - Produce a detailed plan and a series of DR tests for each LA Service

  - Identify a scenario for DR test which ensures the integrity of business data is maintained at all times during the test.

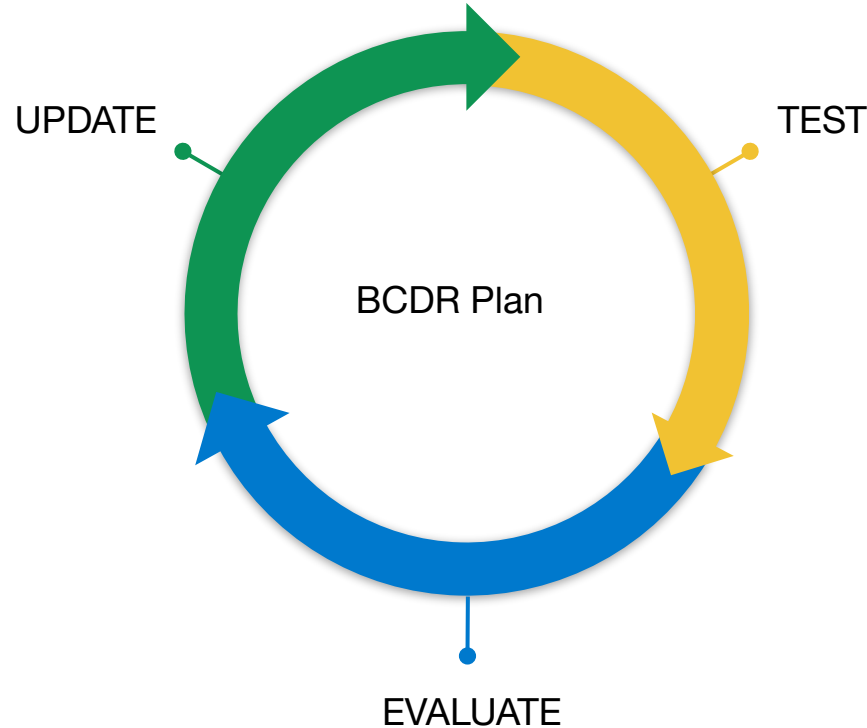LOCAL DIGITAL | Cyber

How to perform a BC/DR test

● Take a staged approach cont'd:

  – Perform configuration checks on DR infrastructure to ensure all are configured and built correctly.

  – Ensure that the DR test plan for each IT service includes fail over to the secondary DC and switching back to the primary DC

  – This plan must include service readiness checks to ensure service is operational

LOCAL DIGITAL | Cyber

How to perform a BC/DR test (cont.)

Regularly test your plan in a realistic way to make sure it works.

- Full Proven test
  - Plan and perform a test failover(s) and switch back, which just proves the recovery capability, with basic service checks run on the DR service.
  - Note: be prepared to repeat this exercise increasing level of test assurance each time.
  - Repeat Full Proven test after each major infrastructure change.
- Full Operational test
  - Plan and perform full failover and run the business service for an agreed period from the DR Data Centre.
  - Repeat this Full Operational at least every 12 months

LOCAL DIGITAL | Cyber

BC/DR continuous improvement cycle

Thank you

[We welcome feedback on our cyber support service](#)

🐦 **@LDgovUK**

www.localdigital.gov.uk

#LocalDigital   #FixThePlumbing

LOCAL DIGITAL Cyber