Overview of RTO & RPO

V1.1

LOCAL DIGITAL Cyber

Objective

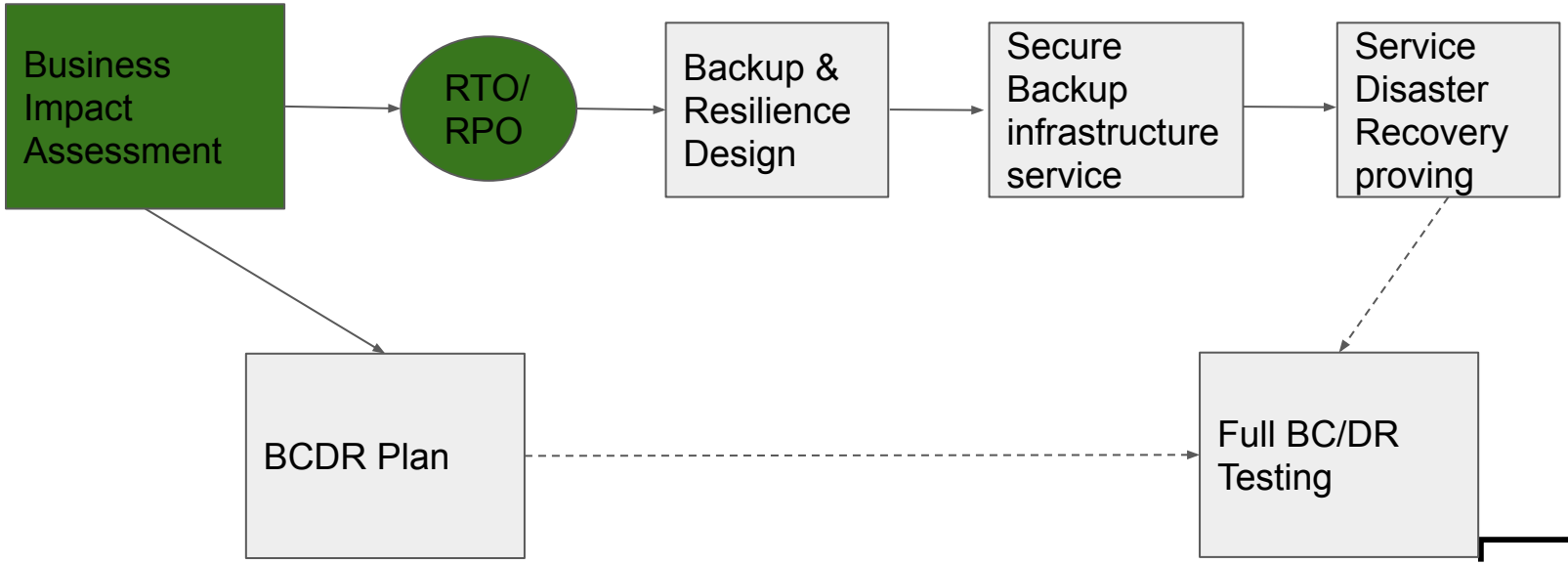
- Outline guidance and approach to enable RTO and RPO target definition for all Local Authority council information systems.
- This is in response to Objective 1 in the Building Resilience in Local Governments – Final Report, dated May 2020 which states:

  “In the majority of local authorities, a short-term solution of backing up critical systems and data to ensure organisations are able to regain control after an incident.
- A common, enterprise-grade , backup solution utilising cloud technology, encryption and multi-factor authentication … to provide a consistent and approved process would significantly assist in the reduction of these risks.”
- Defining RTO & RPO figures support LAs ability to recover more quickly following a ransomware attack or a disaster

LOCAL DIGITAL Cyber

CTP Connections

Mission Critical service resilience and recovery.



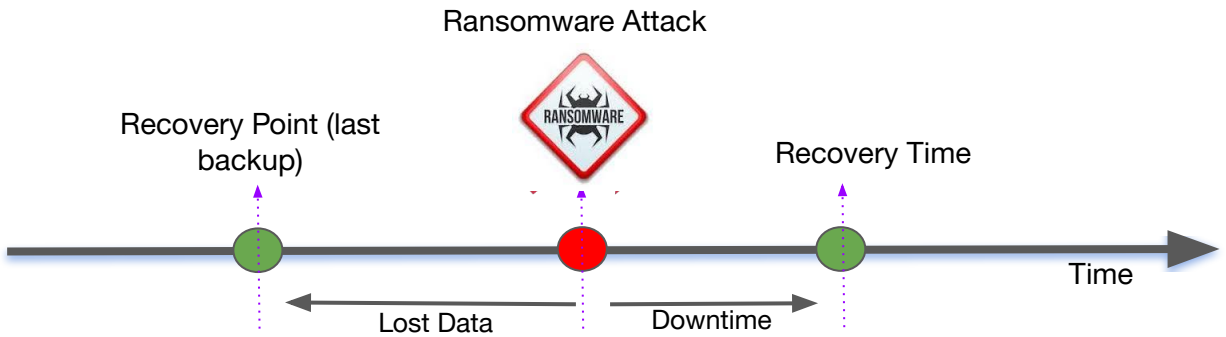
LOCAL DIGITAL Cyber

RTO & RPO definition

RTO: the measure of how quickly the LA is able to restore an application service

RPO: the measure back in time to when data was last saved in a usable format (usually the most recent backup)

i.e. how much data you can afford to lose since the last backup?



LOCAL DIGITAL Cyber

Why are they important?

They are:

- an agreed level of risk exposure of a disaster or ransomware attack to the IT service for the business
- the recovery time from loss of service due to ransomware attack or other disaster
- the targets agreed between the business service owner and the IT organisation
- a key Service Level

They drive:

- the underlying network and IT infrastructure design, IT service design and resilience for the business service
- the backup frequency and processes for restoration
- they contribute to the BCDR Planning so the business can have a clear view of recovery activities and their dependencies

LOCAL DIGITAL Cyber

How to define an RTO & RPO?

- They are an agreed outcome from a Business Impact Assessment (BIA) for each area of the business.

BIA overview

- A BIA is designed to analyse and predict the consequences of a disruption to a business process and the criticality of the service to the organisation.
- It provides critical information required to provide recovery priorities, strategies for the BCDR Plan including RTO & RPO.
- It highlights the impact to the LA (and their customers) of the loss of a business process or service from both a monetary and reputational perspective.

LOCAL DIGITAL Cyber

Recommendation

- Produce BIA for each LA service that are agreed by service owners and ratified at senior level.
- By clearly defining RTO and RPO you will be able to strike a balance between disaster preparation and cost efficiency which is right for your organisation.
- The resulting RTO & RPO should be used as key target for BCDR testing for each service.
- Do not assume IT is automatically available. In a disaster all services should be assumed to be unavailable.

LOCAL DIGITAL Cyber

BIA areas for consideration

- A BIA does not just cover ICT. It should cover all business areas, their functions, the impact of their not being available and the length of time that can be withstood before their restoration.

- Typical areas to be considered for inclusion in a BIA are:

- **Monetary Impact:**

  The “Monetary Impact" of a failure must be considered in terms of both revenue lost and expenses incurred to the specific area concerned (not the whole council)

LOCAL DIGITAL Cyber

BIA Areas for consideration (cont.)

Non-Monetary Impacts:

- Impact to staff or public wellbeing
- Damage to, or loss of, premises, technology, or information
- Breaches of statutory requirements
- Breaches of regulatory requirements
- Damage to reputation
- Deterioration service quality
- Environmental damage
- Premises e.g. what critical functions are run from each building

LOCAL DIGITAL Cyber

BIA areas for consideration (cont.)

- Critical ICT Applications/Software e.g.
    - Application name
    - Critical function
    - Purpose of use
- Vital Records- Paper / Electronic
- External Vendors, Suppliers, Contractors etc. Dependencies
- Special Equipment / Plant / Vehicles

LOCAL DIGITAL Cyber

BIA areas for consideration (cont.)

Telecommunications requirement

- For example, any critical / unique telephone numbers required to perform critical functions)

Minimum staff requirements

- For example, how many staff members will be required to continue operations within a given time frame?

Worker relocation workstation requirements

- For example, face to face contact with public required

LOCAL DIGITAL Cyber

Cyber resilience BIA

Pro-Forma - Cyber Resilience BIA

LOCAL DIGITAL Cyber

Ministry of Housing,
Communities &
Local Government

Thank you

We welcome feedback on our cyber support service

@LDgovUK

www.localdigital.gov.uk

#LocalDigital #FixThePlumbing