Department for Levelling Up,
Housing & Communities

IT Disaster Recovery (ITDR) Plan and Process Guide

V1.0

LOCAL DIGITAL Cyber

Introduction

- IT Disaster Recovery (ITDR) management is the ability to react to ITDR events in a controlled, pre-planned manner.
- The aim of this plan is to support all Councils to implement and maintain an ITDR plan. This plan is split up into four sections:
  - Gathering the requirements needed to shape an ITDR plan.
  - Guidance on writing an ITDR plan.
  - Testing an ITDR plan.
  - Training and awareness.

LOCAL DIGITAL Cyber

Relationship to Response and Recovery Planning

- ITDR includes planning for resumption of applications, data, hardware, communications (e.g. IT networks) and other IT infrastructure, which distinguishes it from Business Continuity planning.

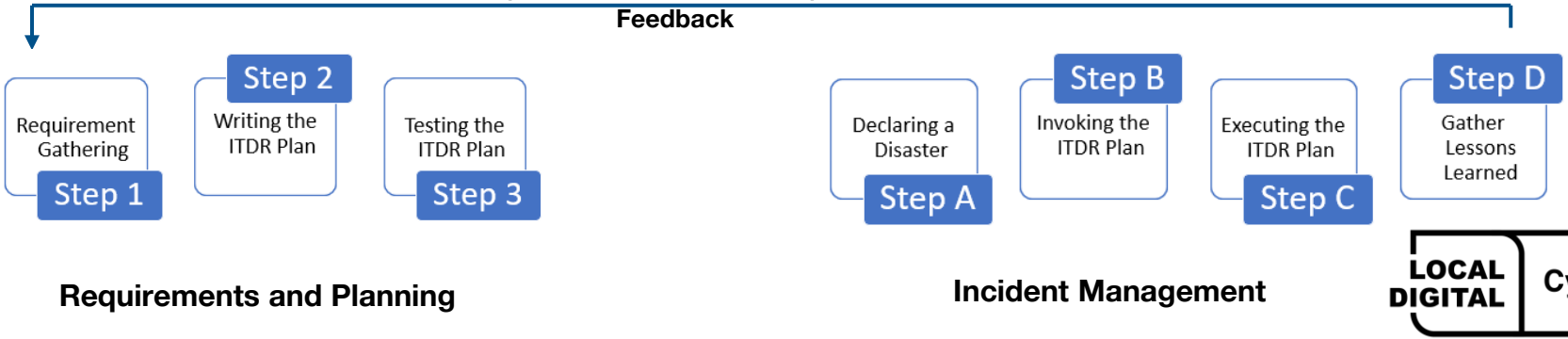
- The Business Continuity Plan (BCP) is broader than the ITDR in that it puts in place a plan for the recovery of an entire Council's business operation in the event of a disaster.

- An ITDR plan is created to;
  - aid the Council in returning to normal operations as quickly as possible.
  - ensure the causes of a disastrous event are captured and understood.
  - help avoid similar incidents in the future; and
  - aid the improvement of the ITDR planning.

LOCAL DIGITAL Cyber

Process

- A good ITDR plan can be summarised into two stages:
- Stage 1: “Requirements and Planning” establishes the requirements for the plan.
- Stage 2: “Incident Management” - to ensure that:
  - incidents are managed appropriately
  - plan is executed effectively
  - lessons learned are captured for future improvements.



ITDR Requirements

- **The Recovery Time Objective (RTO)** is the maximum business-tolerable time that an IT system can be unavailable.
- Must be considered from the Council's point of view where the RTO covers the entire period from initial failover to successful restoration of the Council's operations.
- **The Recovery Point Objective (RPO)** is the amount of data loss which can be tolerated by the Council after a system failover.

LOCAL DIGITAL Cyber

Information Gathering

The following provides details on the base set of information sources required to support the development of an ITDR plan.

ITDR Asset Register

- IT systems subject to the ITDR planning process must be captured in an ITDR asset register.
- Capture the RTO and RPO for each individual IT system.

Business Impact Assessment (BIA)

- Business Impact Assessment (BIA) is carried out for each IT system identified.
- BIA considers what impact would occur to the business in the event that the IT systems were unavailable or data were lost.

LOCAL DIGITAL Cyber

Writing an ITDR plan

This section provides guidance on writing an ITDR plan and each sub-section is an element of the ITDR plan.

IT System Description

- An IT system is the collection of applications and supporting infrastructure which provides IT services.
- List the IT systems, as well as details of the business processes each supports.

Site List

- Details of all primary and secondary physical sites relevant to the recovery process.

LOCAL DIGITAL Cyber

Writing an ITDR plan – Continued…

Dependencies

- A list of dependencies (internal and external) must be included in the ITDR plan.
- Restoration of a business process may be more complex than restoration of a single IT system.
- The impact of the dependency must be captured, in terms of risk, time and cost.
- This information can be used in a disaster event to provide an accurate estimate time for recovery.

LOCAL DIGITAL Cyber

Writing an ITDR plan – Continued …

Internal Dependencies

Dependencies which may materialise as part of the recovery actions, for example:

- When a step in the plan must be completed before a subsequent step can be taken, such as restoring access to a database before conducting login testing.
- If the data centre is in a remote part of the country, and so it may take time for staff to reach the location.

External Dependencies

Dependencies which may affect the success of an ITDR plan, for example:

- Where a previous service, such as power, communication or sanitation facilities, must be restored before a system can be restored.
- Where the recovery of a system must be completed before the Incident Management team can notify staff to return to work at some location.

LOCAL DIGITAL Cyber

Writing an ITDR plan – Continued …

Invocation

- The ITDR plan does not need to be invoked in its entirety. A disaster event may not require the invocation of all the procedures in the plan.
- This section must list those with authority to invoke the ITDR plan.
- Provisions must be made to inform the correct staff of the need to begin recovery procedures.
- IT supplier staff may require a different form of notification, and therefore this procedure should be clearly noted in the ITDR plan.
- Information on individuals who hold the roles listed above should be recorded and kept in an annex.

LOCAL DIGITAL Cyber

Writing an ITDR plan – Continued …

Recovery Procedures

- This section of the ITDR plan must list the functions of the IT system and the business processes it supports.
- Functions should be categorised (into primary and secondary functions) allowing for critical business processes to be restored ahead of others.

Primary Functions

- The primary functions are the business-centric and mandated processes which must be restored for the business to successfully complete its work.

Secondary Functions

- Secondary functions should be restored only after all the primary functions are restored.

LOCAL DIGITAL Cyber

Writing an ITDR plan – Continued …

Recovery Actions

- This section of the ITDR plan should list any actions which are to be used in the recovery effort, and where possible should be cross-referenced with the relevant primary and secondary functions.

- It is recommended that the ITDR plan contains a high level set of actions (e.g. recover file server) with technical details contained in a referenced work instruction or pre-existing operational procedures document.

LOCAL DIGITAL Cyber

Writing an ITDR plan – Continued …

Review

- The ITDR plan is a constantly evolving document, and therefore must be subject to change control and review.
- This section of the ITDR plan must define those responsible for the reviews, as well as the conditions under which the review must be undertaken.

LOCAL DIGITAL Cyber

ITDR Plan Testing

This section outlines the steps required to develop an effective approach to ITDR testing. There are five main approaches to testing an ITDR plan:

- Paper-based testing.
- Walkthrough testing.
- Component testing.
- Parallel testing.
- Cutover testing.

LOCAL DIGITAL Cyber

ITDR Plan Testing – Continued …

Paper-based testing

- Collects together all of the available documentation for the system.
- Examine the documented processes and interviews with staff, to ascertain whether all of the necessary provisions exist to meet the recovery requirements for that IT system.

Walkthrough testing

- Non-technical, real-time test involving a role-play exercise where all relevant stakeholders walk through an ITDR scenario.
- All resources need to be available and set aside to test a specific scenario, these include business staff and IT staff.

LOCAL DIGITAL Cyber

ITDR Plan Testing – Continued …

Component testing

- Test individual components of the processes and technology.
- Component testing provides an opportunity to gain confidence that the individual components of the IT system can be restored successfully.

Parallel testing

- Testing involves the use of hardware which has been sourced or set aside for the purposes of testing.
- Essentially, this form of test is operating a full restoration of an IT system in a non-live setting. In this type of testing, the ITDR process is run in parallel alongside the live system.

LOCAL DIGITAL Cyber

ITDR Plan Testing – Continued …

Cut-over testing

- Focuses upon putting a disaster recovery system into a live setting.
- This involves the complete dependence on the backup system rather than the primary.
- It is strongly recommended that all previous types of tests are considered and reviewed.
- Care must also be taken to ensure that the live service is not affected during the setup and execution of this test.
- Appropriate service or maintenance windows are identified and agreed with the business, in order to minimise risk to business operations.

LOCAL DIGITAL Cyber

ITDR Plan Testing

Objectives

- IT services can be recovered after an incident.
- IT continuity provisions can minimise the impact to the Council and their operations, in response to an incident.
- The ITDR procedures for a return to ‘business as usual’ operations are validated.
- Additional factors, such as communication, and incident and alert management are sufficiently robust.
- To allow staff to become familiar with the ITDR plan.

LOCAL DIGITAL Cyber

ITDR Plan Testing

- Test results must show:
  - Gaps in the level of service.
  - Actions to address these gaps must be identified and assigned to owners.
- A consolidated report for management should be complied, in order to illustrate the results of the tests, along with actions taken to address any issues that arose.
- The process of examining the results against the requirements should identify ‘defects’ in the Plan documentation and process. These defects must be identified and fed back into the planning documents.

LOCAL DIGITAL Cyber

ITDR Plan Testing

Success criteria

A test can only be declared a success if the following conditions are met *:

- The Council processes which are covered by the ITDR plan are proven to be recovered to working use at the end of the test period.
- The entire IT system, including data, can be accessed by users within the period of time specified by the agreed RTO limit.
- Where applicable, users can access the IT system from a necessary site after the failover has been tested.
- The amount of data loss can be specified exactly, and is within the RPO limit.

*** Note:** *This is not an exhaustive list.*

LOCAL DIGITAL Cyber

ITDR Plan Testing

Review and update

- Subsequent review of the test must be undertaken to ensure that all test results are reflected in the ITDR plan.
- Any unexpected results arising from the test, which have not been rectified or are still outstanding issues, are document in the ITDR plan including any actions to rectify any defects or issues.

LOCAL DIGITAL Cyber

ITDR Incident Management

The following table provides a generic set of incident management steps.

STEP	NAME	DESCRIPTION
A	Declaring a Disaster	An incident is declared a ‘disaster’ which requires the ITDR plan to be invoked.
B	Invoking the ITDR plan	The Recovery Team Lead identifies the critical resources and puts forward a communications strategy.
C	Executing the ITDR Plan Procedures	The scope and extent of the disaster is assessed and the ITDR plan is executed following the set of recovery procedures set out in the plan.
D	Status Updates	Regular communication points are recommended to keep the Council updated.
E	Incident Resolution	Once the IT system is considered restored to a sufficient level, a final communication to indicate completion should be made to the Council.
F	Review Results	Lessons learned from the recovery procedure must be reviewed and addressed. These results will establish if the aims and objectives were met and whether the response to the outage was sufficient.

LOCAL DIGITAL Cyber

ITDR Training and Awareness

- All staff should be subject to training in order to raise an awareness of the ITDR plan and their individual roles within it.
- Ensure staff and their departments know what to do in the event of an incident and how they will be impacted.
- Business requirements should be communicated to staff and accommodated within the ITDR plan.

LOCAL DIGITAL Cyber

Staying in touch

Follow our progress

- Read our fortnightly sprint notes on Medium
- Follow LDCU on Twitter (@LDgovUK)
- Subscribe to our Cyber newsletter for progress updates and news relevant to those working in and around local government cyber security
- We'll also be sharing regular updates on the DLUHC Digital blog

Have your say

We welcome further collaboration and input, so if you would like to share with us any strong evidence to support our research please email cybersupport@localdigital.gov.uk.

LOCAL DIGITAL Cyber

Department for Levelling Up,
Housing & Communities

Thank you

We welcome feedback on our cyber support service

@LDgovUK

www.localdigital.gov.uk

#LocalDigital #FixThePlumbing

LOCAL DIGITAL Cyber