# An ICT Disaster Recovery Blueprint for Local Authorities

### January 2025

**Contents**

[Tables and Figures 3](#_Toc187323631)

[About our Blueprint Series 4](#_Toc187323632)

[Glossary 5](#_Toc187323633)

[1. Introduction 6](#_Toc187323634)

[1.1. Who should use this Blueprint? 6](#_Toc187323635)

[1.2. How should this Blueprint be used? 6](#_Toc187323636)

[2. ICTDR: A Definition 8](#_Toc187323637)

[2.1. What is ICTDR? 8](#_Toc187323638)

[2.2. ISO definition 8](#_Toc187323639)

[2.3. Intended meaning 8](#_Toc187323640)

[3. ICTDR: The Wider Context 9](#_Toc187323641)

[3.1. Understanding Business Continuity Management 9](#_Toc187323642)

[3.2. ICT as an enabler 9](#_Toc187323643)

[3.3. Visualising Business Continuity Management 9](#_Toc187323644)

[3.4. Start with corporate Business Continuity Management 10](#_Toc187323645)

[3.5. Business Impact Assessment 11](#_Toc187323646)

[3.5.2 Assisting the wider council 12](#_Toc187323647)

[3.6. Bringing it all together 13](#_Toc187323648)

[3.7. Useful frameworks 15](#_Toc187323649)

[4. ICTDR: Designing Solutions 16](#_Toc187323650)

[4.1. A strategic approach 16](#_Toc187323651)

[4.2. Inputs and dependencies 16](#_Toc187323652)

[4.3. Planning considerations 16](#_Toc187323653)

[4.4. Outputs 17](#_Toc187323654)

[4.5. A worked example 18](#_Toc187323655)

[5. ICTDR: Invoking a Disaster Recovery Plan 30](#_Toc187323656)

[5.1. Invoking plans 30](#_Toc187323657)

[5.2. DR operational planning 30](#_Toc187323658)

[5.3. Returning to BAU 31](#_Toc187323659)

[5.4. Returning to Business Not-As-Usual (‘New Normal’) 31](#_Toc187323660)

[6. Validating and Verifying 32](#_Toc187323661)

[7. Key messages 36](#_Toc187323662)

[Appendix 1: ICTDR Solutioning Checklist 37](#_Toc187323663)

# Tables and Figures

[Table 1: Worked example of ICTDR 14](#_Toc187243982)

[Table 2: Notes on Table 1 (worked example) 18](#_Toc187243983)

[Figure 1: Business Continuity Management System 8](#_Toc187244021)

[Figure 2: ICT’s role in BCM 11](#_Toc187244022)

[Figure 3: Exercising 23](#_Toc187244023)

[Figure 4: Exercising scenarios to consider 24](#_Toc187244024)

[Figure 5: Maintenance and review 24](#_Toc187244025)

# About our Blueprint Series

The Local Government Association (LGA) has developed a series of blueprints to support councils in England with cyber defence and resilience. They bring together a set of essential points to consider in managing, detecting, defending against and minimising the impact of cyber incidents. Each blueprint has been produced in line with the National Cyber Security Centre’s (NCSC) [Cyber Assessment Framework](https://www.ncsc.gov.uk/collection/caf/cyber-assessment-framework).

With the cyber threat landscape rapidly evolving, it is more important than ever that councils have robust strategies and plans in place to detect and respond to cyber-attacks. Our blueprints are intended to help councils with managing, and protecting against, cyber threats. We encourage councils to embed cyber resilience planning at strategic and operational levels to ensure the continuous delivery of critical services if and when a cyber incident occurs.

**Overview of Blueprint series**

No two councils are the same: each face different challenges within their respective environments. Our Blueprints, listed below, provide general guidelines for building strong cyber strategies to improve resilience that can be tailored to local contexts.

* [Cyber security and resilience blueprint series | Local Government Association](https://www.local.gov.uk/our-support/cyber-digital-and-technology/cyber-security-and-resilience-blueprint-series#:~:text=This%20blueprint%20has%20been%20developed,(NCSC)%20Cyber%20Assessment%20Framework.)

We recommend reading our Blueprints in conjunction with each other. If you would like to arrange a conversation with the LGA team about cyber resilience, please email [cyberanddigital@local.gov.uk](mailto:cyberanddigital@local.gov.uk)

**Disclaimer**

This ICT Disaster Recovery Plan Blueprint for Local Authorities provides general guidelines and should be used as a reference. It is not a legal document and may not take into account all relevant local and national considerations. The LGA assumes no legal liability that may arise from the use of this document.

# **Glossary**

BAU Business as Usual

BC Business Continuity

BCP Business Continuity Plan

BCM Business Continuity Management

BCMS Business Continuity Management System

BIA Business Impact Analysis

CIA Confidentiality, Integrity, Availability

DR Disaster Recovery

ICT Information and Communications Technology

ICTDR Information and Communications Technology Disaster Recovery

ISO International Organisation for Standardisation

MTPD Maximum Tolerable Period of Disruption

MBCO Minimum Business Continuity Objective

RPO Recovery Point Objective

RTO Recovery Time Objective

# **1. Introduction**

## 1.1. Who should use this Blueprint?

This Blueprint is aimed at ICT professionals working in councils in England. We suggest using it to facilitate dialogue with colleagues to ensure a joined-up and well-understood approach to cyber planning and DR implementation measures. This includes working with the following people to ensure that ICTDR plans are invoked in line with the council’s overarching BCMS.

* BCM colleagues.
* Emergency planning colleagues.
* Any service for which BC planning is a legal duty.

ICT professionals working in councils can read through this guidance and familiarise themselves with ICT’s role within the council wide BCMS.

## 1.2. How should this Blueprint be used?

This Blueprint provides guidance explaining the typical Business Continuity Management System within a council, including the essential processes and procedures councils must undertake to fulfil their BC responsibilities. The guidance has four sections:

* ICTDR: A definition.
* ICTDR: The Wider context.
* ICTDR: Developing solutions.
* ICTDR: Invoking a DR plan.

At the end of this document, in Appendix 1, we provide a template to assist ICT teams in gathering the service-specific information required to design solutions for DR in line with this guidance. This can support the overall readiness of ICT functions in the area of DR.

We recommend using this guide alongside our [‘Business Continuity Plan’ Blueprint](https://www.local.gov.uk/our-support/cyber-digital-and-technology/cyber-security-and-resilience-blueprint-series) to build a fuller picture of BCM a council-wide perspective – and the role ICT plays i.e. through its development of solutions and plans to invoke DR.

# 2. ICTDR: A Definition

## 2.1. What is ICTDR?

There is no single definition of ICTDR. Indeed, it has become increasingly poorly-defined as a term. In some parts of the world, ‘Disaster Recovery’ and ‘Business Continuity’ may be used interchangeably. Online explainer videos, frameworks and workbooks offer differing interpretations and when vendors offer ‘DR solutions’; they often speak of ‘resilience’.

## 2.2. ISO definition

For this guide, we use the definition below. This International Standard covers an area slightly wider than this document, and we recommend you review the newest edition of it, which will be published in 2025. Our Blueprint breaks down the elements of the statement below, setting out the obligations of a council, and specifically ICT, in delivering to the requirement.

*“Ability of the ICT elements of an organisation to support its critical processes and activities to an acceptable level within a predetermined period of time following a disruption.”*

Source, ICT Disaster Recovery, ISO/IEC DIS 27031 (2024)

## 2.3. Intended meaning

BC and ICTDR are both concerned with ensuring an organisation can **continue** to operate in the case of an adverse event. The protocols they layout support an organisation in swiftly restoring its operations to normal (or ‘new normal’). The two are distinct but interdependent functions. Therefore, processes and solutions should not be developed in silo.

# 3. ICTDR: The Wider Context

## 3.1. Understanding Business Continuity Management

BCM is an important process for developing council wide-resilience. A BCM ‘process’ or ‘system’ should comprise policies and procedures, developed by BC and Emergency Planning teams, to enable key services to continue in an adverse event. They should be promoted across the entire council. All functions or ‘teams’ within a council should undertake a BIA within their service area to identify the critical functions needed to continue. As a distinct workstream within a council, ICT teams also need to carry out their own BIA.

## 3.2. ICT as an enabler

With council services becoming increasingly digitalised, it is important to recognise the role played by ICT as a key enabler for services across a council to continue operating when confronted by an adverse event. Identifying resource dependencies is crucial to any BCMS. Therefore, understanding DR through the lens of BC is critical.

## 3.3. Visualising Business Continuity Management

Figure 1 illustrates the key steps in a BCMS and its relationship to ICTDR. A detailed breakdown of this figure is provided in this guide. We recommend reviewing the diagram below in conjunction with our ‘Business Continuity Plan’ Blueprint.

**Figure 1: Business Continuity Management System**

The business continuity management thread contains a flow chart outlining the key stages of a business continuity management process. The steps in this process are:
• Establishing the objectives of Business Continuity Management and its associated structure.
• Ensuring the organisations is culturally aware and engaged.
• A council wide Business Impact Analysis should be undertaken by the different business areas including ICT which run its own services - such as its Service Desk. There is also a funnel pointing to the Business Impact Analysis step indicating that ICT service management should carry out a BIA along with other business areas. This also highlights that ICT also runs 'foundational services' - like 'the network' which need to be considered as part of the wider BCP planning process.
• The next step is prioritisation and establishing timelines for restoring services.
• Once those fundamentals are established, the process for designing BCM solutions and assigning roles is undertaken. These are then subsequently implemented by developing plans and response structures.


The role of ICT thread shows an overview of the stages where ICT feeds into BCM and vice versa therefore highlighting the interdependencies. The main steps shown are:
• How ICT has to build BC and DR into its overall strategy
• How ICT must inform risk assessments and Business Impact Analyses undertaken in the wider organisation - and how it has to do those itself
• How ICT co-designs DR solutions with the business as well as considering DR for its own foundational services.
• This ultimately leads to a coordinated, cross team approach if there is an 'event' that necessitates for the invocation of the Business Continuity plan and ICT Disaster Recovery

## 3.4. Start with corporate Business Continuity Management

In order to be a success, every organisation should have an overarching framework for Corporate Business Continuity Management, which fulfils the elements shown on the *left box* in the above diagram. Through a process of risk assessment and prioritisation, the organisation should identify its key services and the likely business impacts caused by an adverse incident.

Below, we outline a set of key considerations to help build the foundations of BCM, acknowledging ICT’s role within it.

* **Leadership and Culture:** BCM is an organisational-wide issue, requiring management support. It should be established as a formal concept in the organisation with associated roles. Considering BC should become a part of organisational culture.
* **Risk and Impact:** Service areas, **including ICT**, should conduct a Business Impact Assessment to assess the risks to their service, processes and activities and the likely impact on them resulting from a negative event.
* **Mitigation and Restoration:** Service areas, **including ICT**, should determine the need for their services to mitigate against likely risks, and make clear their priorities for restoration of an appropriate level of function and the required timelines for restoration (known as DR).
* **Prioritisation:** A council should consider overall prioritisation, as it will have a limited amount of resource and not everything can be ‘Priority 1’. Tough decisions will be required, and many areas may have to accept a lower priority than they might desire, including the lowest.
* **Solutions:** Solutions should be developed to deliver necessary continuity, and roles established. This will include ICTDR elements (see section 4 for further detail). Solutions should be accompanied by plans and response structures. These approaches should be validated, tested/exercised, and improved on as required.

## 3.5. Business Impact Assessment

The role of BIA cannot be understated for all areas of the council, especially ICT. In any council, ICT is a core function, providing essential support across the entire organisation.

ICT must

* Consider its **own internal** critical operations which need to continue in a period of disruption and then establish a solution for this accordingly.
* Work with **council-wide service areas** to identify which services are dependent on ICT and co-design appropriate solutions.

To clarify, however, and for the sake of removal of doubt, business continuity planning for other business services is **not** vested in IT. This is the responsibility of Corporate Business Continuity Management, and the individual service area directors.

**3.5.1 Analysing ICT’s internal operations**

The services provided by ICT typically cover 1) ICT service management and 2) the provision and maintenance of foundational technologies.

**ICT service management:** ICT must maintain a line of communication and service with end users. Thus, as part of business continuity planning, ICT should consider its processes for maintaining this service in a period of disruption. This will have a side benefit for corporate business continuity – who will need to communicate, and will require points of contact.

**Foundational technologies:** ICT must also identify its ‘foundational’ services, systems and assets that underpin its ability to maintain its own processes. Additionally, it must consider those elements which underpin basic delivery of safe ICT services to users.

For example, these might include:

* Authentication, Authorisation and Accounting (AAA)
* Communications (incl. voice, messaging, email)
* Core network (incl. network security and access)
* Internet connectivity and/or cloud
* Managed end user devices
* Partner connectivity
* Service desk
* Virtualised platform

For these services, and informed by business requirements, ICT must consider the need for those assets to be protected, initially, against risks such as attack and failure, plus their arrangements for DR solutions in the event that things do go wrong.

## 3.5.2 Assisting the wider council

All service areas within the council must undertake BC planning. They will also have critical dependencies on internal or external ICT functions. ICT should work with teams from the outset to ensure services understand how resilient their systems are and help them explore solutions for disaster recovery.

ICT should either be involved in identifying these dependencies either as a delivery partner, or by providing internal knowledge and expertise to teams. Without this involvement, it is likely that key elements will be missed.

While it is ultimately up to the service what resilience or recovery requirements it may need, ICT and relevant suppliers must set out workable, relevant costed options so that the service area may make an informed choice.

ICT and suppliers should ensure that the limitations, as well as the benefits of such solutions are made clear to the service. This includes the potential for data loss, and how major events might impact on timeliness of actions.

## 3.6. Bringing it all together

Once the BIA has been undertaken within ICT, and core dependencies have been identified across other services, ICT should work with teams across the council to co-design solutions for that service.

They should also work with Business Planning and/or Emergency Planning teams to inform the design of BCM solutions, for which ICT considerations are essential. Plans and tests for invoking DR can then be prepared (see Figure 2).

**Figure 2: ICT’s role in BCM**

A diagram of a software development

Description automatically generated

BCM requirements should be embedded in an appropriate **policy and approach**, which ICT leadership support. As part of this, ICT should ensure that its approach is consistent with wider BC planning.

ICT leadership must ensure that adequate, competent resources are available, and that overall responsibility for this area is also assigned.

In summary, ICT and ICT suppliers must:

* Consider their own BC requirements.
* Mitigate against risks to solutions, their own and those of the business, including contributing to the resilience of those services.
* Develop DR solutions and plans for their own foundational services.
* Co-design elements of business services, mitigate risks and build DR plans and solutions for the wider organisation.
* Test and validate plans and solutions.
* Enact plans in an appropriate priority order in the event of single system/solution failure or in the case of a wider incident.

## 3.7. Useful frameworks

The [ITIL v3 Service Lifecycle, or the ITIL v4 Practices](https://www.axelos.com/for-professionals/my-axelos) are useful frameworks to refer to, and can support ICT teams in understanding how to plan and implement incident, problem and change management during an event.

As an example, ICT should consider:

* **Incident and Problem Management**: How will the chain between service users and ICT be maintained during disruption? How will activity be coordinated in ICT?
* **Change Management:** Controlling what is changed, how and by who is a vital part of maintaining service stability and continuity. Disruption can require multiple non-standard changes being undertaken at high speed. To avoid chaos, who will be in charge, and what rules will need to be followed?

# 4. ICTDR: Designing Solutions

## 4.1. A strategic approach

As part of a strategic approach to setting DR procedures, ICT needs to consider inputs and dependencies, planning considerations, resources, and the outputs it needs. We provide in this section guidance and templates to assist ICT teams in co-designing solutions for DR under the lead of BC teams, as well as considerations for testing, validating, and enacting DR plans.

## 4.2. Inputs and dependencies

Required resiliency and specific DR solutions should be informed by:

* **Risk assessments and BIAs:** These should be derived from BC planning within services areas. (Equivalent assessments should also be undertaken as part of ICT Service Management and security activity.)
* **A prioritisation plan:** Pre-identify with the organisation’s leadership team the priority services and activities where resources will be directed first in the case of an adverse event.
* **An assessment of existing levels of resilience:** Assess existing DR solutions and the organisation’s view on their reliability and efficacy (‘assurance’). Note that, where documentation and plans for this do not exist, they should be created in line with organisational standards.

## 4.3. Planning considerations

ICT should collaborate with the appropriate service area lead (or wider business continuity group/equivalent) to plan appropriate DR solutions where there is ICT resource dependency. This involves consideration of:

* **Invoking plans:** How and when DR solutions may need invoking.
* **Resourcing:** What skills and knowledge are required accounting for constraints such as staff availability, shifts, absence planned and unplanned.
* **Timeframe:** At what point appropriate **levels** of service may need to be restored, and by when they **must** be restored:
  + **MBCO:** This is the minimum level of service needed by the business to deliver its basic required functions in a disaster.
  + **RTO:** This is the point in time by which that level should be achieved.
  + **MTPD:** This is the point at which business disruption will exceed what can be tolerated.
* **Tolerance:** The organisation’s **tolerance** for data loss, and loss of integrity where relevant.
* **RPO:** The point in time to which data can be recovered i.e. if this is two days previous, then two days’ worth of data will be lost.
* **Recovery options:** The reality of options available and likelihood these will enable recovery in line with the desired RTO. (Note that, the introduction of solutions and plans should not introduce new, unmanaged risks.) This should include an assessment of:
  + The **cost** of options – bearing in mind that solutions should not usually exceed the costs of the impact on the organisation.
  + The **assurance** of those options – security, reliability etc.
* **Standards and resources:** Reference should be made to any beneficial standards and knowledge resources when choosing different types of solutions.

## 4.4. Outputs

When using the considerations outlined in 4.3, the following outputs are recommended:

* Agreed and signed-off DR Solutions.
* Agreed and signed-off Response and Recovery plans for the invocation of those solutions, including relevant triggers, roles, responsibilities, and how the invocation will be communicated.
* Test plans for the above, and a testing schedule.
* Inputs to the wider BC process.

## 4.5. A worked example

Below, we provide a worked example, and explanatory notes, of an ICTDR that can be used to drive discussions and log decisions. A downloadable version of this is available in Appendix 1.

**Table 1: Worked example of ICTDR**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ICTDR solutioning checklist** | | | | | 01.01.2025 | | | |
| *Scope of DR requirement* | | Legacy Network Attached Storage (CENTRA) | | | | | | |
| *Assessment performed by* | | J P Simmonds | | | | | | |
| *Description/purpose of system:* | | CENTRA is our legacy in-house Network Attached Storage solution. It stores our ‘home folders’ (Z:\), and provides file system storage for legacy SharePoint and the DUCK planning solution. | | | | | | |
| *Third party involvement:* | | Internal ICT Service Provider, *‘MBOX’*. | | | | | | |
| **A: Summary of any existing resilience arrangements : Confidentiality, Integrity, Availability (C, I, A)** | | | | | | | | |
| *Risk being protected against: (plus C,I,A)* | Local Disk Failure (IA) | | *Likelihood:* | High | | | | |
| *Impact:* | Data loss to any impacted data, any users. | | | | |
| *Solution:* | Drives configured for redundancy (RAID), hot-swap. | | | | |
| *Assurance Level:* | HIGH | | System is monitored automatically, alerts generated, business processes in place. | *Last test:* | 20.12.2024 |
| *Recovery Time Objective* | Zero | | *Recovery Point Objective (How much data can be lost)* | Zero | |
| *Actions:* | None | | | | |
| *Risk being protected against: (plus C,I,A)* | Full single site loss (A) | | *Likelihood:* | Medium | | | | |
| *Impact:* | Complete loss of NAS storage due to physical site failure (e.g. fire) | | | | |
| *Solution:* | Data live mirrored to NAS on secondary site, automated failover | | | | |
| *Assurance Level:* | MEDIUM | | System has failed over, but not formally tested for 4 years. | *Last test:* | 01.03.2021 |
| *Recovery Time Objective* | 1 minute | | *Recovery Point Objective (How much data can be lost)* | Zero | |
| *Actions:* | Plan for a test in next 3 mo. Assigned to JS, 01.01.2025 | | | | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *Risk being protected against: (plus C,I,A)* | | | Power failure, single site (A) | | | | *Likelihood:* | | | Medium | | | | | | | | | | | | | | |
| *Impact:* | | | Complete loss of NAS storage due to single site power failure | | | | | | | | | | | | | | |
| *Solution:* | | | UPS coverage both sites 2.5 hours. Resilient against single site loss. | | | | | | | | | | | | | | |
| *Assurance Level:* | | | LOW | | | No formal testing.  UPS shows 1x battery fail | | | | | | | *Last test:* | | | | ??.??.???? |
| *Recovery Time Objective* | | | Zero | | | *Recovery Point Objective (How much data can be lost)* | | | | | | | Zero | | | | |
| *Actions:* | | | URGENT: Review suitability of current measures. Assigned JC, 01.01.2025 | | | | | | | | | | | | | | |
| **B: Consideration of new DR and Resilience Requirements** | | | | | | | | | | | | | | | | | | | | | | | | |
| *Risk scenario being protected against* | | | Ransomware encryption & data loss – assuming any/all areas of storage | | | | | | | | | | | | | | | | | | | | | |
| *What would ‘impact’ look like?*  *i.e. what impacts are we attempting to control.* | | | * Data would be encrypted or damaged beyond repair. * The system on which data was stored might not be readily recoverable due to forensic investigations. * Existing backups using our live mirroring would also be corrupted. * Service area work would be disrupted, and ICT resource diverted to managing the incident. * An attacker might cause damage before any obvious attack. | | | | | | | | | | | | | | | | | | | | | |
| *Impacts:* | | | *Area* | *Business purpose impacted* | | | | | | *Tolerable RTO from BCPs* | | | | *Tolerable RPO from BCPs* | | | | | *Maximum Tolerance (MTBD)* | | *Proposed solution number* | | | |
| ALL | Home folders | | | | | | 3 weeks | | | | 2 days | | | | | 3 months? | | 1 | | | |
| ASC CSC | Legacy SharePoint storage – general working papers outside of case system | | | | | | 1 days | | | | Zero | | | | | 2 weeks? | | 1 | | | |
| Planning | All planning activity requiring case management | | | | | | 5 days | | | | Zero | | | | | Not considered in BCP | | 2 | | | |
| **C: DR Solutioning** | | | | | | | | | | | | | | | | | | | | | | | | |
| *Solution ID* | 1 | Name: | | | Veribak immutable backup (cloud, UK) with Microsoft 365 secondary tenant (cloud). | | | | | | | | | | | | | | | | | | | |
| Description of functionality: | | | The Veribak solution mirrors our online storage and configuration (incl. user accounts). A file history is maintained, and up to 3 months of changes to files can be recovered. This is a lower cost solution, as such there is a lead time on recovery of 1 day.  A secondary Microsoft tenant, with minimal licensing requirements, could be built up swiftly and grown as a ‘safe space’ for our staff to work in, and we could recover files and data to there if we were to lose our internal systems. | | | | | | | | | | | | | | | | | | | |
| Simple description of DR invocation: | | | In the event of an incident, we would determine if it was safe to restore files from VeriBak to our existing infrastructure. If this could not be proven ‘clean’, we would restore files to the secondary tenant and set up users on there as part of a wider business continuity effort. | | | | | | | | | | | | | | | | | | | |
| Timeliness: | | | RTO | | | 1 day | | | RPO | | | | Zero | | Max Tolerance | | | | | 3 months | | |
| Managed risks/impacts? Avoids new risks? | | | Yes.  Introduction of supplier requires assurance. | | | | | | | | | | | | | | | | | | | |
| Does the plan meet the needs of all service areas/processes which it covers? | | | No  It is likely that ASC/CSC data would take 2 days to make available, rather than one. This requires discussion with ASC/CSC. | | | | | | | | | | | | | | | | | | | |
| Resource requirements on invocation? | | | Financials to increase tenant licensing if required - £AAAA  2-3 staff for 3 days to restore and build tenant. Comms and training for staff to use tenant. | | | | | | | | | | | | | | | | | | | |
| Costings | | | £NNNN/year. | | | | | | | | | | | | | | | | | | | |
| Time to implement: | | | 2 months | | | | | | | | | | | | | | | | | | | |
| Alternate options | | | The business may wish to consider moving these files to a cloud solution with these elements built in. Costs of this would be £VVVV/year. Migration would take 4 months. This would allow us to remove our legacy storage, saving £XXXX/year and would provide more predictable costs. | | | | | | | | | | | | | | | | | | | |
| Third parties consulted: | | | Yes | | | | | | | | | | | | | | | | | | | |
| Business agreement: | | | TBC | | | | | | | | | | | | | | | | | | | |
| Agreement to proceed: | | | TBC | | | | | | | | | | | | | | | | | | | |
| **C: DR Solutioning** | | | | | | | | | | | | | | | | | | | | | | | | |
| *Solution ID* | 2 | Name: | | | | DUCK online | | | | | | | | | | | | | | | | | | |
| Description of functionality: | | | | Move from our legacy hosted infrastructure to the online hosted version of DUCK. | | | | | | | | | | | | | | | | | | |
| Simple description of DR invocation: | | | | From initial assessment, it appears that the DUCK online solution meets the resilience requirements of the business. As such, these arrangements would be handled by DUCK | | | | | | | | | | | | | | | | | | |
| Timeliness: | | | | RTO | | | 2 day | | | RPO | | | | Zero | | Max Tolerance | | | | | ???? | |
| Managed risks/impacts? Avoids new risks? | | | | Yes – but assurance will be required from the supplier. | | | | | | | | | | | | | | | | | | |
| Does the plan meet the needs of all service areas/processes which it covers? | | | | Yes – but assurance will be required from the supplier. | | | | | | | | | | | | | | | | | | |
| Resource requirements on invocation? | | | | This will be handled by the third party. | | | | | | | | | | | | | | | | | | |
| Costings | | | | £NNNN/year. | | | | | | | | | | | | | | | | | | |
| Time to implement: | | | | 3 months? | | | | | | | | | | | | | | | | | | |
| Alternate options | | | | Upgrade internal DUCK solution, noting this would still remain on legacy storage, which has reliability issues. | | | | | | | | | | | | | | | | | | |
| Third parties consulted: | | | | No. An assessment of the system and assurances given by supplier is required. | | | | | | | | | | | | | | | | | | |
| Business agreement: | | | | Initial discussions made. | | | | | | | | | | | | | | | | | | |
| Agreement to proceed: | | | | TBC | | | | | | | | | | | | | | | | | | |

**Table 2: Notes on Table 1 (worked example)**

|  |  |
| --- | --- |
| **Scope:** | Any assessment of requirements needs a clear **scope**. While this could be a complex service (including a ‘network’), or even a specific piece of technology as per the example above, it’s important that the scope is manageable – if an analysis is looking too complex, you should consider, is the scope too big? |
| **Third parties:** | It’s important to determine any third parties and supply chain responsibilities up front – they will need to be involved in, and considered in the analysis. |
| **Section A: Summary of existing resilience arrangements** | |
| **Existing arrangements:** | It is important to determine what existing resilience arrangements are present, whether it is effective, and whether it is sufficient. This aligns to the ‘gap analysis’ performed as part of wider BC planning. |
| **Risk being protected against (CIA)** | **What risk scenarios have been considered?** Do they protect against issues of Confidentiality, Integrity (accuracy/fitness for purpose) or Availability. In considering *Likelihood and Impact,* you should refer to your organisation’s risk management framework for definitions and – depending on scope – consult with impacted areas of the organisation.  **What assurance do you have in the current solution?** Does it work well? Use this as an opportunity to take stock. In particular, and if relevant, when did you *test* it last?  **What Recovery Time Objective (RTO)** **does the solution attempt to deliver?** What is the organisation’s tolerance to the system or service being unavailable? You should compare this to what the business expects in its BC plans (RTO), and what it can tolerate (MTPD).  If information and data is involved, is there a risk of data loss? If so, how much data might feasibly be unavailable? As a simple example, if data was backed up every two weeks, there’s a risk – if restoring – that up to two weeks data could be lost. The figure here gives you the current **Recovery Point Objective** – which again should be checked to see that it is sufficient for business.  (Note: For a *ransomware* attack or similar, this figure could be larger – imagine in the example above that you retain data for two months – but the attacker is in your network for three, and you can’t trust the backups you have.  You might need to assign **Actions** to conduct further reviews |
| **Section B: Consideration of new DR and Resilience Requirements** | |
| **Scenario:** | What threats or risks need to be protected against? Depending on your findings and the effectiveness of existing solutions, it may be worthwhile re-reviewing those already defined in Section A. However, the aim here should be to take on board relevant risks defined in other locations, for example:   * Corporate Risk Register entries relevant to the solution. * Relevant risk registers of departments. * Identified risks to Business Continuity from BC Planning. * Identified Cyber Security risks. * Identified ICT risks.   Likelihood and impact should be pre-defined in those locations, so these are not considered directly here, but you should refer to them in business discussions. |
| **Impact description:** | It’s vital that the impact of any scenario is explained clearly when determining solutions. This impact should be discussed with non-ICT managers and staff. |
| **Impacts** | What Business Areas of the organisation might be impacted? What elements of their business, or things that they rely on might be affected?  How soon might they need to be backed up and working to a basic level even if it is not to the normal operational standards? This is likely to be their **Recovery Time Objective**.  How much data could they lose in normal circumstances? This may be their **Recovery Point Objective.**  Given everything, what’s the maximum time they could cope with before things become intolerable? This would be the **MTBD.** If considering a ***ransomware*** attack, where data that has been previously backed up might be impacted – you should make sure that this potential loss of data has been considered. |
| **Solution** | From your considerations, you may propose a number of solutions. These are referenced here and expanded on in the next section. |
| **Section C: DR Solutioning** | |
| **Name and description** | For your solution(s), it’s important to set out what they are, in a language that can be explained to the wider business. |
| **DR invocation** | Also, in plain language – what would you do if you had to invoke the solution? This leads to your DR plan (see part 3 of this document) |
| **Timeliness** | What is the anticipated RTO/RPO. What length of business disruption does the solution attempt to insure against? |
| **Risks and Impacts covered and not introduced?** | Solutions need to manage the risks and impacts for which they have been designed. If not, or if there are weaknesses, it’s important to declare these, so they can be understood by management.  It’s also vital that new, unmanaged risks aren’t introduced – e.g. for a resilient solution, is there sufficient distance between elements to avoid failure in case of a physical incident? |
| **Needs met?** | It may be possible that solutions available don’t meet the needs of everyone who they might cover. Such areas of non-coverage need to be discussed and agreed with the relevant line of management. It may be that the solution needs to be re-engineered, or that risks may have to be accepted by leadership. |
| **Costings:** | How much will it cost? Costs of solutions should generally not exceed the cost of risk impact. |
| **Time to implement:** | How long might it take to implement the solution? It’s rare that solutions have no lead time – and the business may want to discuss its prioritisation. |
| **Alternate options:** | The obvious option may not be the best option – so it may be of benefit to lay out others for the business to consider. As an example, adding resilience to an existing system may be less effective than replacing it; building solutions for two individual systems might be less effective than a solution that can be used for both. |
| **Sign-offs:** | It’s important that third parties are consulted, and agreements are in place.  In addition, ICT management should only sign off a solution if:   * Its implications and resource needs are understood: people, facilities, technology, information, finance and reliance on / need for suppliers. * The solution is aligned with the Business Continuity needs of the organisation. * The solution is aligned with the organisation’s risk appetite. * The solution is aligned with the organisation’s legal, regulatory, and contractual obligations. * Plans to implement and invoke solutions will be co-ordinated by nominated individuals. * The plans shall include testing wherever feasible to determine their effectiveness, and the efficacy of the planned solution. |

# 5. ICTDR: Invoking a Disaster Recovery Plan

## 5.1. Invoking plans

DR solutions are invoked during a disaster. They are automated, infallible, and transparent (e.g. the ‘disaster’ is averted 100 per cent of the time). They are likely to be part of a chain of response, which will require careful handling. Invocation of DR solutions must be **planned**, and as such, considered in advance and documented as a plan.

As solutions exist to enable the continuity and recovery of business, we encourage you to discuss these requirements with the relevant BC professionals in your organisation.Ideally, DR plans and solutions should form part of the wider BCMS, which should have influenced their creation and requirements from the start.

## 5.2. DR operational planning

Below are just some of the elements to consider in your operational planning. As BC frameworks typically include these elements and more, we do not attempt to replicate relevant documents here, but encourage you to refer to existing frameworks such as those provided by the Business Continuity Institute (BCI) and in part by our ‘Business Continuity Planning’ Blueprint.

* **Scenario:** When would DR be invoked?
* **Authority:** Whoor what decides to invoke it, under what authority?
* **Consequence:** Who wouldbe impacted in a time of decreased/limited service?
* **Communication:** Who will be informed, by who, with what messaging? How will that be managed over time?
* **Logging:** How will records be maintained of the event?
* **Relationship:** Is invocation likely to be linked to a wider BC incident – or might it cause one? Which other teams need to be informed and involved? (BCP, Emergency Planning, cyber security etc.)?
* **Monitoring:** How will you know that things are going as planned?
* **Efficacy:** How will concerns with the effectiveness of the solution be received and responded to whilst it is in operation?
* **Availability:** How will your plans be available for you to follow? Are there dependencies on other elements (e.g. networks, services, solutions) that might impact your ability to invoke DR if they were affected at the same time?

## 5.3. Returning to BAU

Your plans for invoking DR should include plans for closure – **when** is DR no longer required, **who** decides? These plans and processes should be documented. If your organisation has a template for operational plans of this type, it should be used. You should consider items such as:

* Returning to primary resources from alternate ones.
* Handling long-term unavailability of resources.
* Priorities – what will resume and when? Will a return to BAU take priority over restoring any lower-priority services (as determined in BC planning)?
* Will new vulnerabilities be introduced?

A decision on **when** and **how** to return to BAU is required – as a successful return requires the correct resources to be available, and the return to be phased correctly. It may be that you have external dependencies which enable or prohibit return – for example the involvement of regulatory or security bodies, or insurance terms and requirements.

## 5.4. Returning to Business Not-As-Usual (‘New Normal’)

In developing plans and processes for returning to BAU, you may consider that a return to the ‘as-was’ state is either not desirable or not feasible. For example, from a physical perspective, if ICT equipment is destroyed, you are unlikely to be able to re-use it.

As such, it is acceptable and encouraged to consider whether a ‘new normal’ is likely to be required. Notwithstanding this scenario, plans for returning to BAU are likely to be tested heavily during a ‘real life’ scenario – and leadership will need to make active decisions based on circumstances to ensure a successful approach.

# 6. Validating and Verifying

Good practice typically recommends that management undertake specific activities to ensure that continuity practices and processes are verified for efficacy, and remain effective long term – and these apply equally to ICTDR. These include:

* **Exercising:** Evaluating capability, testing and validating solutions and processes, verifying the adequacy of resources to deliver them, validating roles and responsibilities, building confidence (see Figure 3 and Figure 4).
* **Maintenance:** As BAU, incorporating organisational and environmental changes to ensure that processes and plans remain effective (see Figure 5).
* **Review:** Obtaining and building assurance that solutions and processes are effective.

**Figure 3: Exercising**

|  |
| --- |
| How do you know your plans will work? Will DR be activated appropriately? Will the necessary resources be available and will the relevant personnel know what to do? Exercising and involving relevant areas of the organisation as required is vital to offer you assurance and the opportunity to review your processes. Below, are some principles that may assist in designing and developing a suitable programme:   * **Exercises should be part of a planned programme of assurance**: ‘Ad hoc’, unplanned exercising rarely occurs – day-to-day priorities take over. * **The Exercise programme should be owned**:A competent individual should be in charge on behalf of management to assure that ICT’s plans are exercised and tested. * **Management should seek assurance on the programme:** Reporting on testing completions and any issues discovered must be highlighted to ICT management – and the wider business through BC discussions, if relevant. * **Exercise methods:** A number of approaches can be taken – from discussing plans, through scenario exercising (‘tabletop’), through simulations and tests. When choosing a mechanism:   + Considerations should be made of the efficacy of the method – e.g. a discussion on an ICT ‘failover’ function is less likely to be useful versus testing the failover itself.   + Considerations should be made of the impact of exercising on the business, especially where testing is performed on live services. If there is any risk of disruption, the wider organisation must be involved in the process.   + The objectives of exercising, and any outputs, should be agreed in advance. |

**Figure 4: Exercising scenarios to consider**

|  |
| --- |
| Using scenario tests, involving the wider business through BC planning, can be a good way to test the **scope** of your DR plans. For effective exercising, we strongly recommend co-ordinating with BCP colleagues. As an example, consider the following specific complex scenario, accompanied by some specific elements to consider.  *As the result of a ransomware attack, all of our end user devices have been put out of service. While our BCP means that we have cloud services we want to direct our users to, we have no clean devices for them to use at present. It’s also the weekend.*   * What is our approach to recovering from this disaster? Have we planned for it? * What resources do we have in place, or need to obtain to deliver our plan (funding, technology, available and competent personnel)? * Would we have financial backing if we needed to spend? How would we obtain funds? * Do we have a plan or process to guide those resources? * Would the plan be timely and effective? Would it meet the wider business need? * Does the plan consider the risk of devices being re-infected? * Who do we deliver devices to first? Is this impacted by specific business needs at this point in time? * How might we accelerate this if we needed to? * How would we deliver this if there were multiple competing priorities? |

**Figure 5: Maintenance and review**

|  |
| --- |
| Maintaining ICT’s approach to DR is vital for success. As a simple example, a change to infrastructure configuration, or a resource restructure which fails to take account of DR and continuity plans can result in them being rendered useless at the time of impact.  Management should ensure that maintenance and review activities are planned and assigned. A management review of ICTDR effectiveness should be scheduled to validate that maintenance occurs and is effective. Maintenance and review are part of a wider cyclical approach.  **Review types:**   * Changes to ICT services, infrastructure, and configuration (from *Change Control)*. * Changes to ICT resources and skilling. * Changes to external suppliers and systems. * Lessons learned from exercises, events and incidents. * Changes to organisational structures and activities. * Changes to the external environment, threats and risks. * Results of management reviews and independent audits. * Obsolescence of approach e.g. unsupported solutions. * Availability of improved approach e.g. new solutions. * Changes to organisational BC and digital needs and priorities. |

# 7. Key messages

The purpose of this document has been to define and understand ICTDR – including how to develop solutions and plans – through the lens of wider Business Continuity. It has been designed to be used by any council, regardless of its maturity in the area. Our key messages are:

* Effective functioning ICT ultimately exists to support the digital goals of local government. It supports the continuous delivery of services to residents, local businesses, and communities by councils.
* While it is possible to look at ICTDR elements in isolation – particularly when considering specific ‘foundational’ ICT functions and technologies – we encourage you to not do so unless absolutely necessary.
* All services ultimately exist to service the need of the organisation and the community that it supports, and participation in wider BC planning will ensure that DR elements are effectively specified, aligned, tested and appreciated. Looking at DR from the wider BCP angle increases the likelihood of them being funded.
* We encourage ICT teams to support the development of Wider Business Continuity Planning in your organisation, as it is likely to deliver direct benefits to ICT in this area.

# Appendix 1: ICTDR Solutioning Checklist

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ICTDR solutioning checklist** | | | | | DD.MM.YYYY | | | |
| *Scope of DR requirement* | |  | | | | | | |
| *Assessment performed by* | |  | | | | | | |
| *Description/purpose of system:* | |  | | | | | | |
| *Third party involvement:* | |  | | | | | | |
| **A: Summary of any existing resilience arrangements : Confidentiality, Integrity, Availability (C, I, A)** | | | | | | | | |
| *Risk being protected against: (plus C,I,A)* |  | | *Likelihood:* |  | | | | |
| *Impact:* |  | | | | |
| *Solution:* |  | | | | |
| *Assurance Level:* |  | |  | *Last test:* |  |
| *Recovery Time Objective* |  | | *Recovery Point Objective (How much data can be lost)* |  | |
| *Actions:* |  | | | | |
| *Risk being protected against: (plus C,I,A)* |  | | *Likelihood:* |  | | | | |
| *Impact:* |  | | | | |
| *Solution:* |  | | | | |
| *Assurance Level:* |  | |  | *Last test:* |  |
| *Recovery Time Objective* |  | | *Recovery Point Objective (How much data can be lost)* |  | |
|  |  | | *Actions:* |  | | | | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *Risk being protected against: (plus C,I,A)* | | |  | | | *Likelihood:* | |  | | | | | | | | | | |
| *Impact:* | |  | | | | | | | | | | |
| *Solution:* | |  | | | | | | | | | | |
| *Assurance Level:* | |  | |  | | | | | *Last test:* | | |  |
| *Recovery Time Objective* | |  | | *Recovery Point Objective (How much data can be lost)* | | | | |  | | | |
|  | | |  | | | *Actions:* | |  | | | | | | | | | | |
| **B: Consideration of new DR and Resilience Requirements** | | | | | | | | | | | | | | | | | | |
| *Risk scenario being protected against* | | |  | | | | | | | | | | | | | | | |
| *What would ‘impact’ look like?*  *i.e. what impacts are we attempting to control.* | | |  | | | | | | | | | | | | | | | |
| *Impacts:* | | | *Area* | *Business purpose impacted* | | | | *Tolerable RTO from BCPs* | | | *Tolerable RPO from BCPs* | | | *Maximum Tolerance (MTBD)* | | *Proposed solution number* | | |
|  |  | | | |  | | |  | | |  | |  | | |
|  | | |  |  | | | |  | | |  | | |  | |  | | |
|  | | |  |  | | | |  | | |  | | |  | |  | | |
| **C: DR Solutioning** | | | | | | | | | | | | | | | | | | |
| *Solution ID* | 1 | Name: | | |  | | | | | | | | | | | | | |
| Description of functionality: | | |  | | | | | | | | | | | | | |
| Simple description of DR invocation: | | |  | | | | | | | | | | | | | |
| Timeliness: | | | RTO | |  | | RPO | | |  | Max Tolerance | | | |  | |
| Managed risks/impacts? Avoids new risks? | | |  | | | | | | | | | | | | | |
| Does the plan meet the needs of all service areas/processes which it covers? | | |  | | | | | | | | | | | | | |
| Resource requirements on invocation? | | |  | | | | | | | | | | | | | |
| Costings | | |  | | | | | | | | | | | | | |
| Time to implement: | | |  | | | | | | | | | | | | | |
| Alternate options | | |  | | | | | | | | | | | | | |
| Third parties consulted: | | |  | | | | | | | | | | | | | |
| Business agreement: | | |  | | | | | | | | | | | | | |
| Agreement to proceed: | | |  | | | | | | | | | | | | | |
| **C: DR Solutioning** | | | | | | | | | | | | | | | | | | |
| *Solution ID* | 2 | Name: | | |  | | | | | | | | | | | | | |
| Description of functionality: | | |  | | | | | | | | | | | | | |
| Simple description of DR invocation: | | |  | | | | | | | | | | | | | |
| Timeliness: | | | RTO | |  | | RPO | | |  | Max Tolerance | | | |  | |
| Managed risks/impacts? Avoids new risks? | | |  | | | | | | | | | | | | | |
| Does the plan meet the needs of all service areas/processes which it covers? | | |  | | | | | | | | | | | | | |
| Resource requirements on invocation? | | |  | | | | | | | | | | | | | |
| Costings | | |  | | | | | | | | | | | | | |
| Time to implement: | | |  | | | | | | | | | | | | | |
| Alternate options | | |  | | | | | | | | | | | | | |
| Third parties consulted: | | |  | | | | | | | | | | | | | |
| Business agreement: | | |  | | | | | | | | | | | | | |
| Agreement to proceed: | | |  | | | | | | | | | | | | | |