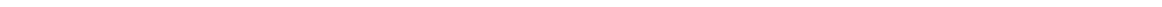




ICT Business Continuity & Disaster Recovery for Local Authorities

White Paper



Contents

| | | |
|-----|--|---|
| 1 | Introduction | 3 |
| 1.1 | What Constitutes a Disaster?..... | 3 |
| 1.2 | Phases..... | 3 |
| 1.3 | Overall Contingency Planning | 3 |
| 2 | Discovery Phase | 4 |
| 2.1 | Audit and Analysis | 4 |
| 2.2 | Service Prioritisation..... | 5 |
| 2.3 | Business-As-Usual Service Management | 5 |
| 2.4 | BC/DR Analysis | 6 |
| 2.5 | BC/DR Action Plan & Recommendations..... | 7 |
| 3 | Design Phase | 8 |
| 4 | Implementation Phase | 9 |
| 5 | Support Phase | 9 |
| 6 | Offer and Contact Details..... | 9 |

1 Introduction

Most councils recognize that the drive towards electronic government inevitably increases reliance on ICT and hence increases the risks and impacts of failures in supporting systems. Similarly, the rate of change in the use of ICT means that a full inventory review and overhaul of contingency plans must become a regular process rather than a once-off event. Also, most councils will already have an overall plan and management structure in place to deal with major catastrophes. We focus specifically on BC/DR for ICT and networks and aim to plan and provide cost-effective solutions to assure business continuity within that framework. This short paper describes the approach we have successfully adopted in solving local councils' problems and describes the specific services we offer. In particular, we recognize that a major constraint is always cost and a viable solution should not involve a significant levy on the local council tax payers. Hence we can be extremely flexible in how we shape any offer to suit your specific needs.

1.1 What Constitutes a Disaster?

We don't like to be dogmatic on this. Obviously it includes major terrorist outrages and, while a "911" type event may be exceedingly unlikely in your authority, such attacks cannot, unfortunately, be ruled out. Fire, flood, power cuts, gas/chemical leaks, network failures and thefts form the most common set of disaster events. In addition to disrupting ICT, they often have severe consequences in terms of staff and premises. We take all these into consideration in our plans. In terms of minor disasters, BC/DR should merge seamlessly into your normal everyday service management procedures - viruses, machine failures, network outages etc are so commonplace that everyone should already have systems in place to cope with these. Our approach is to ensure that the ICT disaster plan is fully consistent with, and makes as much use as possible of, your existing procedures.

1.2 Phases

Depending on your current situation, BC/DR planning can be a significant piece of work. We have applied our standard project methodology - DDIS (Discover, Design, Implement and Support) – to the BC/DR planning life-cycle to split it into manageable phases. Each can be undertaken by different suppliers chosen according to their expertise for the given phase whilst maintaining overall project integrity. The expertise that MorganDoyle brings to each phase is shown in the table opposite.

| | |
|------------------|---|
| Discovery | Inventory Audit Risk Assessment Impact Analysis Recommendations Options |
| Design | Processes and Procedures Organisation Statement of Requirements |
| Implement | Supplier Evaluation Implementation Project Management Training |
| Support | Exercise & Test Refresh (inventory, processes & procedures) |

1.3 Overall Contingency Planning

We find that most councils already have an overall BC/DR plan in place for civil contingencies. We don't try to re-invent the wheel. Rather, we work within that framework, especially regarding organisational responsibilities, the management team and general areas such as emergency services, physical security, insurance, HR, PR, etc. In particular, during the implementation phase, we ensure that the detailed BC/DR recovery procedures for disasters affecting ICT are consistent with existing Council policies, responsibilities, line management and reporting.

However, the forthcoming Civil Contingencies Bill will impose some additional duties on local authorities and other bodies. If you would like any assistance with overhauling your existing framework or even creating a new overall plan from scratch we may be able to help. Our framework covers the major organisational and managerial issues specific to local authorities, and it can be tailored to suit your local structure and external relationships relatively quickly and cheaply.

A few examples of our approach to engaging with this generic framework might be helpful:

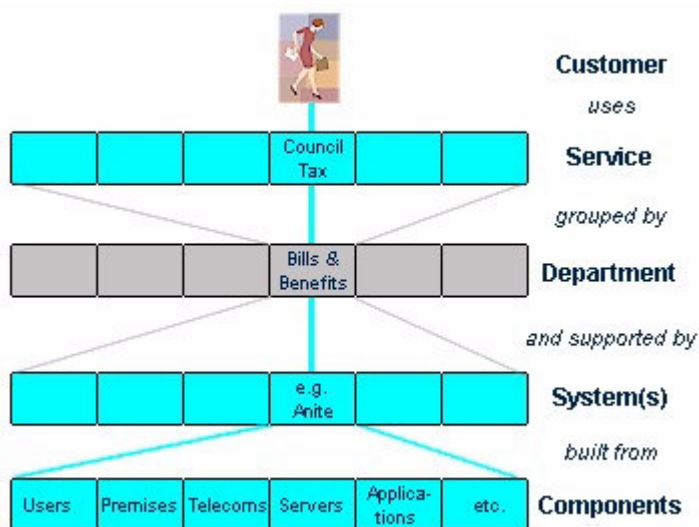
Insurance. As part of the general risk analysis/impact assessment during the discovery we naturally assess the reliance of insurance on ICT systems. More importantly we take on board the role of insurance in the overall DR plan and existing procedures, e.g. liaison to insurance carriers and claims adjusters post-disaster, coordination of insurance cover/premiums with continuity planning programs, etc. This is used during the design and implementation phases to ensure that specific recovery procedures are consistent with the Council's insurance policy.

Human Resources systems are part of our normal risk analysis, impact assessment and mitigation plans. However, since immediate contact to all your staff is vital in any emergency, HR systems also have a special role as they are often the major centralised source for staff contact details. During the design and implementation phases we align detailed procedures with the role of HR in the overall BC/DR plan, e.g. support for the HR elements of recovery, staff notification, etc. post-disaster.

Public Relations systems too are part of our normal risk analysis, impact assessment and mitigation. The role of PR in communication with the news media, public and staff who are not involved in the recovery operation should not be underestimated in managing the emergency. Hence support for PR and it's role in an emergency falls into the design and implementation phases.

2 Discovery Phase

2.1 Audit and Analysis

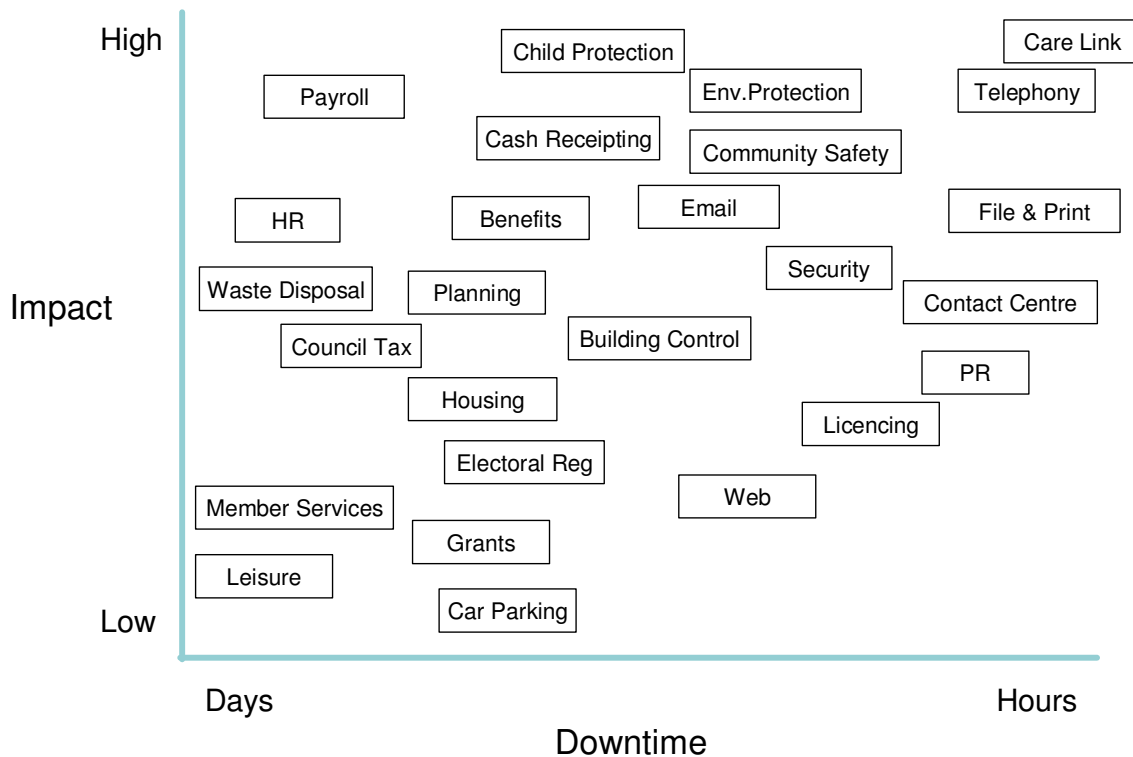


The goal of the initial discovery phase is always to fully understand how the Council's services, both external to its customers and internal to support operations, are supported by ICT systems and all the resources upon which these rely - hardware, software, network, management, staff, premises, etc. We work closely with the ICT department to audit existing systems and procedures. The data is loaded into our "service inventory" database to help identify and analyse risks and single points of failure - if you already have a hardware and software inventory or asset register, importing from this is no problem.

This phase concludes with an interim report identifying immediate risks and recommending concrete, practical actions for risk avoidance and mitigation that can be implemented internally, offering major benefits for minimal outlay.

2.2 Service Prioritisation

One of the most sensitive issues in any Business Continuity plan is service prioritisation; the natural tendency being to classify everything as essential, until the cost of such a solution is appreciated. At this stage in the process, involving a supplier with an incentive to sell the most sophisticated, expensive and probably inappropriate DR solution possible is a positive hindrance. Ultimately, this prioritisation has to come from the customers themselves. In the case of a council this should involve both senior officers and elected representatives. Working "top-down" we hold workshops with senior Council officers and committee chairmen to understand their priorities for service delivery. As independent external advisors we guide this process to help "normalizing" priorities across different services. This is a delicate decision for the council since they must weigh the three major competing impacts – revenue loss, degraded BVPI and public well-being.



One important point to get over is that this prioritisation is not absolute. For example, we do not seek to decide that housing benefit is more or less important than say housing maintenance. Rather, the goal is to understand their relative priorities in terms of how soon one needs to recover from a disaster and what level of recovery is acceptable in the interim. By mapping services onto supporting infrastructure this classification also forms basis for the requirements specification for a BC/DR solution.

2.3 Business-As-Usual Service Management

We ensure that the ICT disaster plan is fully consistent with and makes as much use as possible of your existing investment and merges seamlessly into your normal everyday service management procedures. This applies to data backup, fault management, helpdesk, service assurance & monitoring, UPS etc.

We appreciate that your data is already backed up and we aren't going to try to sell you a costly replacement system you don't need. Rather, during the design phase, we will ensure that post-disaster your media and systems can be reloaded onto the equipment available in an emergency, whether that be a "ship-to-site" solution or a solution hosted in a remote data centre.

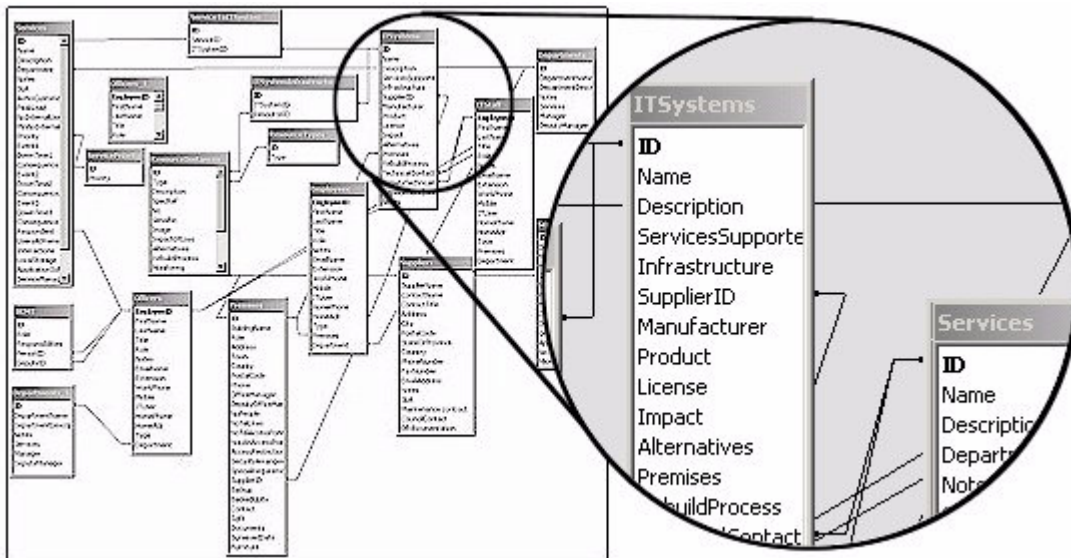
Similarly, standby generators as well as specialist UPS units are standard risk avoidance mechanisms that you may well already have in place. Nevertheless, it is essential to audit test schedules and ensure that invocation of these systems does not have undesirable side-effects.

When a disaster, big or small, occurs, existing fault management systems and helpdesk are likely to be overloaded or may themselves be rendered unavailable. In a sense the BC/DR plan is a replacement of these systems for use in an emergency, e.g. for prioritisation, responsibilities, etc. In smaller scale emergencies the existing FMS may be integrated with the plan.

2.4 BC/DR Analysis

The discovery phase amasses a large amount of information with a variety of highly significant relationships but it is quite useless if you can't manage and manipulate it. We have found that it is the relationships and mappings between services, ICT systems and supporting infrastructure that are key to risk assessment and impact analysis.

Our approach to make this manageable is to load the information into a small database that can be copied and distributed to members of the BC/DR management and emergency teams, so that the information is always available. This core database of shared information supports lookups between systems and allows "What If" scenarios to be run, such as assessing the service impact of a failure at a given location. It is capable of modeling the complex relationships between ICT components, ICT systems and services:



At the end of any BC/DR project this database is one of our deliverables to you. It gives you complete ownership and control of your data, allowing you to update it as your services and systems evolve. Most importantly, it forms the basis of the DR operational plan because it holds all of the significant information you need during an emergency.

In fact, the database has a role in all phases:

- During the discovery phase to assist data gathering and establish the basic hardware, software and service inventory;
- During DR plan preparation and implementation to allow prioritization of service restoration, skeleton staffing levels, etc; and
- During a DR incident (including training/testing simulation) to reference appropriate re-build documentation, contact details for emergency staff and suppliers, further guidance on server restoration prioritisation, etc.

2.5 BC/DR Action Plan & Recommendations

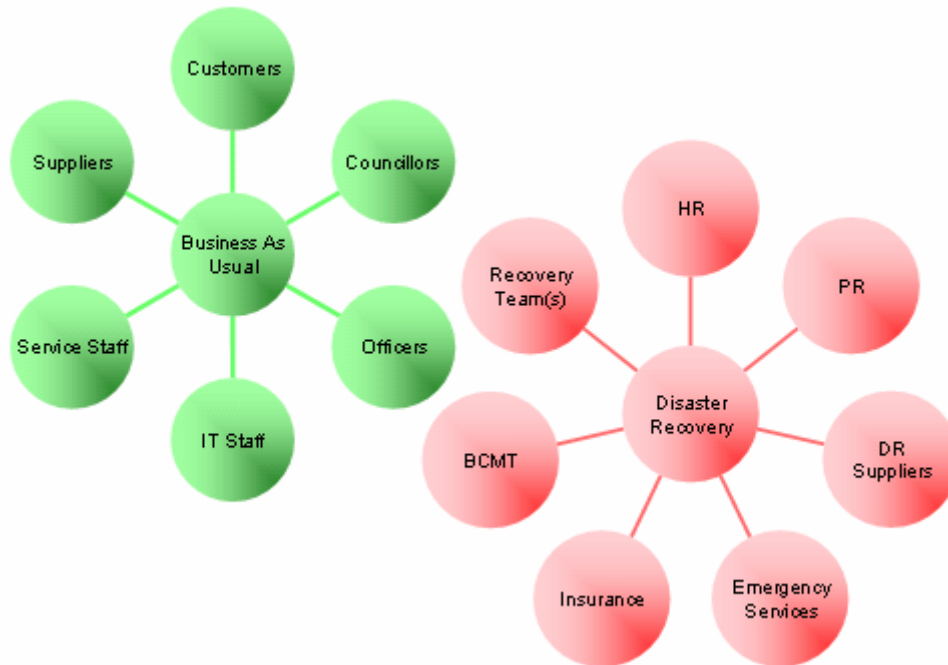
We pride ourselves on giving concrete, practical advice. Another deliverable of the discovery phase is an action plan outlining the major options available to you to plug any holes and assure business continuity. These may include, for example, "ship-to-site" replacement servers and PCs configured to your standard O/S and application builds, loaded with the latest data backup. The Service Level Agreements associated with these are very flexible - banks for example choose to have them available within 2 hours, but then they pay accordingly! We can suggest alternative premises - within your Council, in adjacent councils and/or external data centres and suites for your servers and users made specifically available for this purpose. Since, we are completely independent of all of the DR suppliers we can promise we have no vested interest in the options or your decision.

3 Design Phase

In the design phase the audit information and the chosen recommendations are used to:

- Create the specific Processes & Procedures to be used during everyday business-as-usual activity (to facilitate disaster avoidance / business continuity) and during a disaster to action recovery;
- Specify test regimes;
- Formalise the organisational structure, with roles and responsibilities, for ICT BC/DR and link this into the Council's overall emergency planning hierarchy; and
- Create a formal Statement of Requirements for the BC/DR systems and infrastructure (alternative premises, etc).

We are careful that the design phase focuses as much on people and organization, as it does on the BC/DR ICT infrastructure.



4 Implementation Phase

We back up all our recommendations with the promise that we are prepared to implement them on the basis of a fixed timescale and budget. So if you would like MorganDoyle to be involved in the implementation phase we can:

- Extend the Service Inventory database to include links to contacts and procedures for use in an emergency;
- Manage supplier short-listing (in collaboration with your supplier management/procurement department);
- Assist in the supplier evaluation and selection;
- Manage the implementation by the DR operational supplier;
- Initiate a formal testing regime; and
- Train staff in the processes and procedures.

We do not provide the operational DR facilities (suites, premises, backup equipment etc) - we like to be independent of that.

5 Support Phase

Once the BC/DR plan is operational it should be regularly re-appraised in two respects.

- **Inventory & Process Review.** Changes in the services you offer and your use of ICT means that a full inventory review and overhaul of contingency plans **must** become a regular process - it is not a one-off problem with a one-time solution. There is no compulsion to return to MorganDoyle for this nor is there any implicit lock-in. We provide a full hand-over of all material, data and analyses including the Service Inventory database, giving you complete ownership and control of your data, so you can maintain your BC/DR plan for yourself.
- **Exercising of BC/DR processes & procedures.** Without regular testing of DR/BC infrastructure and practice of the processes by staff, it is unlikely that the BC/DR plan will work well during a real emergency.

We can help with both of these aspects.

6 Offer and Contact Details

We are happy to provide any of these component services in isolation so you can do more or less of the implementation yourselves or with your chosen suppliers. The discovery phase for a BC/DR plan can typically be completed in about 6 weeks.

For further information or advice contact *MorganDoyle* Limited. The latest contact details can be found on our website at <http://www.morgandoyle.co.uk/>