REPORT TO:	**Policy and Resources Committee – 13 February 2006**
REPORT ON:	**ICT Business Continuity/Disaster Recovery Plans 2006/07**
REPORT BY:	**Head of Information Technology**
REPORT NO:	**151-2006**

1.0 PURPOSE OF REPORT

1.1 To outline ICT Business Continuity and Disaster Recovery (BC/DR) Plans and seek Committee approval to proceed with Plans.

2.0 RECOMMENDATIONS

2.1 It is recommended that the Committee approve the proposal in section 8 of this report, to develop a second secure computer facility at 8 City Square for the purposes of ICT Business Continuity and Disaster Recovery.

3.0 FINANCIAL IMPLICATIONS

3.1 Actions proposed in the Plan are provided for in the IT Division Revenue Budget 2005-2008, subject to their approval.

4.0 LOCAL AGENDA 21 IMPLICATIONS

4.1 The IT division has developed and implemented an ICT consolidation strategy which minimises the requirement to purchase and consume ICT resources. This strategy promotes the use of thin client devices which consume less power and have a longer useful life.

5.0 EQUAL OPPORTUNITIES IMPLICATIONS

5.1 During the implementation of I.T. equipment and services, ongoing consideration will be given to the Council's Equal Opportunities Policies in the preparation of any resultant new Divisional practices affecting I.T. staff duties and opportunities.

6.0 BACKGROUND

6.1 The use of Information Communication Technologies (ICT) continues to expand across the Council.

6.2 The Council are investing in public facing electronic services such a self-service on-line services, Customer Contact Centres and provision of high quality ICT in Schools, Libraries and Neighbourhood Centres.

6.3 These increasing demands require reliable, fault-tolerant ICT systems at the core so that disruption of frontline services is minimised. Also, most Council Staff require effective ICT resources to do their job. Disruption to these services for any reason can cause productivity losses and the resultant impact on frontline services.

6.4 There are many external factors which can lead to disruption to ICT services. They include:

- Computer virus, computer 'hacking' or denial of service attacks
- Flood, fire or other environmental impacts which result in evacuation of buildings
- Disruption to mains power supplies or disruption to the Councils wide-area data network
- Civil emergency

6.5 Whilst the above external factors should occur infrequently, they can potentially lead to significant periods of system outage and have a major effect on service delivery. More commonly occurring internal factors listed below tend to have less of a widespread impact on service delivery:

- Hardware or software failure
- Failure of system backups or restores
- Failed upgrade
- Deadlines not met for major project

6.6 Whilst some form of preventative measures are already in place to mitigate all of the above, a more corporate approach to BC/DR has been developed and this report seeks committee approval to implement this approach.

6.7 The approach which is outlined in the next section can only be implemented in a cost-effective manner due to the success of the IT Divisions consolidation strategy. This strategy and the need to implement the strategy is outlined below.

6.8 Historically, ICT systems and service have been developed and implemented for Departmental services, with only systems such as Payroll, Financial systems and latterly e-mail being delivered corporately. This led to often incompatible systems from varying suppliers being installed.

6.9 A systematic strategic approach over the last three years has led to far greater consolidation of systems and services. The Council has consolidated down to two strategic system platforms which facilitate the majority of Council systems and services. Prior to this strategic shift, it has been impractical to consider a large-scale BC/DR deployment as this would mean replicating many different systems from a large range of suppliers.

6.10 Over the last three years, the IT Division has developed and implemented a far more corporate approach to selection, procurement, development and implementation of ICT systems. The reasons for this approach are multi-faceted and are listed below:

- Electronic Service Delivery requires a more corporate approach to service provision

- ICT security threats are managed cost-effectively by hosting all critical services in a secure computer facility

- Managing the requirements of Freedom of Information legislation requires all Council data to be available from a central location

- A crucial requirement when designing the Council's IT infrastructure is the full lifecycle 'Cost of Ownership' of ICT facilities. This is a fundamental consideration

6.11 The above combined approaches, as well as reducing the overall lifecycle costs of ICT have enabled us to propose a cost-effective Disaster Recovery/Business Continuity to serve the needs of both citizens and Council Staff.

6.12 All of these computing systems and servers are currently housed in a secure, environmentally managed Computer Suite at Floor 1, Tayside House. The environment is currently protected against limited loss of power, physical threats, ICT security threats, etc. However, it is recognised that any prolonged loss of this facility for reasons outlined above would have a significant (and increasing) effect on the Council's ability to provide services to its citizens.

6.13 To mitigate these threats, and provide a continuity of service, the Council needs to invest in a second secure, environmentally managed computing facility. Options for this facility have been extensively explored and are detailed in the next section of this report.

7.0 OPTION APPRAISAL

7.1 In order to come up with the most relevant, practical and cost-effective business continuity/disaster recovery solution, a number of options were investigated before deciding on the proposal below. These options are briefly outlined below:

7.2 Do Nothing – This option was appraised on the basis that we already have a level inherent fault tolerance in many of the major systems, but was discounted on the basis that it did not offer a solution to any external issues (listed above) which could impact on the current computer suite.

7.3 Outsource BC/DR – Specialist companies have developed BC/DR offsite computer facilities which can be 'invoked' when certain BC/DR problems occur. This option was discounted due to cost and the impracticality of having to regularly test DCC systems in a remote BC/DR site. Also, there is no guarantee that these facilities would be available when required as other companies and organization pay for a 'share' of the facilities.

7.4 BC/DR 'capacity on demand' – This type of service is offered by manufacturers and can involve Server facilities being provided by a mobile vehicle in the event of major BC/DR problems. The same cost and impracticality reasons as above were used to discount this option as well as the inevitable time delays which would be incurred in setting up this service.

7.5 Second secure computer facility (spare capacity) – This option was seriously considered and is an option that many organizations have adopted. This would involve obtaining and building a second computer suite and installing Systems, Servers etc. which would be configured with Council software and data, but would only be used in the event of BC/DR being invoked. It was discounted on the basis that expensive systems and servers would be purchase but not be used productively.

7.6 Second secure computer facility (live capacity) – This option would be similar to the above option, but the system and server capacity installed in this facility would be used in a production environment to serve up to half of the Council's computer users. Spare storage capacity would be purchased, with ALL data being stored at both computer facilities. In the event of BC/DR being invoked in either of the computer facilities then the other computer facility would serve all of the Council system users. This service provided would not be as high performance, but would allow IT system business continuity. This option is the one that is proposed on the basis of practicality, relevance and cost-effectiveness. Careful consideration of Council plans to move to a new HQ facility has been undertaken. Having this proposed facility in place before the proposed move will ensure that IT Business Continuity can be achieved for the duration of this complex project.

8.0 PROPOSAL

8.1 It is proposed that a second, smaller secure computer facility be developed at 8 City Square. System and server capacity has already been purchased and are currently being used in the Tayside House computer room. Part of this capacity would be moved to the new computer facility.

8.2 Both computer facilities will contain up-to-date copies of all Council data. In the event of a BC/DR problem with one of the facilities or a system failure in one of the facilities then the other facility would serve all Council users until normal service could be resumed. There would be some degradation in performance and in some cases a short delay may be encountered before the new site is serving all users.

8.3 As indicated above, this facility is also required to provide continuity of service during the proposed move to the Council's new HQ. Whilst it is planned to replicate the current Tayside House Computer facility at the new HQ, a second computer facilty will ensure that all systems and services can be available for the duration of the project.

9.0 CONSULTATION

9.1 The Chief Executive, Depute Chief Executive (Finance), Depute Chief Executive (Support Services), Assistant Chief Executive (Management) and Assistant Chief Executive (Community Planning) have been fully consulted in the preparation of this report and are in full agreement with its proposals.

Mr. David White   Head of Information Technology   Date: 31st January 2006