INTERNAL AUDIT REPORT

FROM:	Audit and Risk Manager	**SUBJECT:**	ICT Backup Strategy, Processes and Procedures
TO:	ICT Services Manager ICT Infrastructure Manager Database Administrator	**DATE:**	1 November 2012
C.C.	Chief Executive Head of Finance		

1. INTRODUCTION

1.1 In accordance with the Audit Plan for 2012/13, an examination of the above subject area has been undertaken and this report presents the findings and conclusions drawn from the audit for information and action where appropriate. This topic has previously been audited in October 2008.

1.2 Wherever possible, findings have been discussed with the staff involved in the procedures examined and their views are incorporated, where appropriate, into the report. My thanks are extended to all concerned for the help and co-operation received during the audit.

2. BACKGROUND

2.1 The review focused upon the strategy for computer data backup and recovery of key Council IT systems in operation. In addition, operational processes associated with data backup and recovery has been assessed to determine whether risks are being effectively managed.

2.2 The goal of Computer data backup recovery is to recover data after its loss, be it by data deletion or corruption. Backups are a distinct part of a service continuity management strategy focussing on logical rather physical error.

3. SCOPE AND OBJECTIVES OF THE AUDIT

3.1 The overall objective of the audit is to report a level of assurance for the controls in place to ensure that Council-owned computer data is backed up and can be recovered in a secure and timely manner.

3.2 The audit programme identified the expected controls. The control objectives examined were:

- a backup strategy has been clearly defined that takes into account the time required to backup all key systems and data;
- a process has been established to ensure that all key IT systems and data is backed up as per the strategy;
- data backup is retained for sufficient time to enable a processing cycle to be recreated in the event of any problem arising;

- data backups are retained in a secure environment to ensure that the necessary files can be identified and recovered should the need arise; and
- arrangements for the recovery from backup are in place and are routinely tested for effectiveness.

4. FINDINGS

4.1 Backup Strategy

4.1.1 The ICT Electronic Information Backup Policy has been documented and details the current arrangements for performing computer data backup routines on all Council owned computer data. It has been updated on an annual basis with the last update occurring in September 2012.

4.1.2 Through inspection we confirmed that the Electronic Information Backup Policy refers to the removable media policy. We confirmed that the backup process does not comply with the removable media policy in respect to backup encryption which is not performed.

Risk
Not encrypting backups may lead to breach of data protection legislation and/or reputational damage if backup tapes containing sensitive data are misappropriated.

Recommendation
(1) The ICT Electronic Information Backup Policy should be updated to provide clear guidance as to the Council's approach to backup encryption.

4.1.3 We also inspected the backup elements within the ICT services - Service Area Crisis plan. Service continuity management is covered in more detail in the ICT service continuity management audit reported in March 2012

4.1.4 No further issues were identified under this control objective.

4.2 Backup and Recovery Processes

4.2.1 We confirmed that the Checklist Data Protector Daily Task must be performed during the backup process. This document is signed and dated daily to provide an audit trail that each day’s backup process has been completed successfully.

4.2.2 Roles and responsibilities for the computer data backup and recovery processes within ICT Services have been defined and assigned to officers within the Infrastructure Team. All officers have received training in use of the backup technologies.

4.2.3 The backup process in operation results in computer data being stored on IT application servers, database severs and network storage areas via the software backup solution provided by the third party company, Hewlett Packard.

4.2.4 We confirmed that Windows Active Directory settings are configured to only allow users to save documents onto a network drive. This ensures that Council data is not excluded from the backups process due to storage on local drives.

4.2.5 We confirmed that in the case of a logical failure then transaction logs would be used to restore data. Transaction logs for critical databases are recorded on an hourly basis. In most restore scenarios that do not involve physical damage to server hardware a restore may be completed to a specific point in time. We inspected an inventory of database servers in the form of a server information spreadsheet. This clearly details which database servers are backed up and the backup schedule.

4.2.6 No issues were identified under this control objective.

4.3 <u>Physical Storage of Backups</u>

4.3.1 The backup tapes are written and stored in the server room on level three of Riverside House in a suitably secure environment. Access is controlled via key card access restricted to ICT personnel. Weekly and monthly backups are transported to the town hall each Monday and stored in the fire-proof media safe.

4.3.2 We confirmed that a sequence of tapes are maintained for daily, weekly, monthly and quarterly backups. At the time of the audit we queried the tape retention policy. This has now been increased from 48 to 72 months.

<u>Opportunity</u>
The Council may get better value for money through continuing to keep its tape retention policy under review in light of developing technology.

<u>Recommendation</u>
(2) The Council should build a regular review into their tape retention policy to keep track with developing technology.

4.3.3 No further issues were identified under this control objective.

4.4 <u>Backup recovery</u>

4.4.1 Test restores are tested as part of 'business as usual.' All test restores are recorded on the helpdesk system (Support Works) which was observed during audit testing. We noted that any officer can contact the Help Desk to request data to be recovered.

4.3.3 No issues were identified under this control objective.

5. <u>SUMMARY AND CONCLUSION</u>

5.1 The audit has confirmed that the systems and controls in place to manage the risks associated with computer data backup recovery are generally sound and give SUBSTANTIAL assurance for achieving the objectives as represented in Section 3 above.

5.2 Two recommendations have been made for management consideration relating to backup encryption and tape retention.

6. MANAGEMENT ACTION

6.1 The recommendations arising are reproduced in the attached Action Plan (Appendix A) with management response.

Richard Barr
Audit and Risk Manager

Appendix A

Action Plan

Internal Audit of ICT – ICT Backup Strategy, Processes and Procedures – 1 November 2012

Report Ref.	Recommendation	Risk Rating*	Responsible Officer	Management Response	Target Date
4.1.2	The ICT Electronic Information Backup Policy should be updated to provide clear guidance as to the Council's approach to backup encryption.	Medium	ICT Services Manager	Agreed. The backup policy has been amended to clarify the position on backup encryption for corporate backups, including the addition of a risk assessment. The encryption guidance for all other backups remains valid.	Complete
4.3.2	The Council should build a regular review into their tape retention policy to keep track with developing technology.	Low	Infrastructure Manager	Agreed. HP Data Protector has 'fair' and 'poor' warnings for tapes based on usage and age. Each time a tape goes 'fair' the operating lifespan of the tape will be validated against the suppliers' current best practice for tape retention and usage.	Complete

* Risk Ratings are defined as follows:

Low - Minimal adverse impact on achievement of the Authority's objectives if not adequately addressed.
Medium - Moderate adverse impact on achievement of the Authority's objectives if not adequately addressed.
High - Requires urgent attention with major adverse impact on achievement of Authority's objectives if not adequately addressed.