INTERNAL AUDIT REPORT

GEDLING BOROUGH COUNCIL

IT HEALTH CHECK REVIEW

APRIL 2007

FINAL

CONTENTS

		Page
1.	Executive Summary	2
	Audit Conclusions and Summary	
	Key Issues	
2.	Management Summary of Suggested Action	3
3.	Background, Scope and Objectives.	6
	Acknowledgement	
4.	Findings	
	1 - Responsibilities for controlling the physical security of computing facilities are clearly defined	8
	2 - Adequate precautions exist to protect the IT infrastructure, operating environment and the resources they support	11
	3 - Adequate precautions exist to ensure that data and software is well protected from loss, misuse, theft, damage and accidental or deliberate corruption	14
	4 - Arrangements exist for creating back-up copies of data and programs, storing and retaining them securely, and recovering applications in the event of failure	17
	5 - The transfer of data and IT facilities to and from the organisation is fully secure and third party access to IT facilities is fully protected	18
	6 - Use and Control of the Internet and E-mail	20
	7 – Compliance Arrangements fort the Data Protection Act 1998	22
5.	Assessment of IT Audit Requirements	23
	Appendix A – Suggested IT Audit Plan 2007 – 2009	24

ASSIGNMENT CONTROL:

Debrief meeting:	27 November 2006	Auditors:	Mike Riley, Client Manager Jane Measom-Stevenson, ISA Manager Sheila Pancholi, Senior ISA Manager
Draft report issued:	11 January 2007		
Responses received:	11 April 2007		
Final report issued:	12 April 2007	Client sponsor:	Vince Rimmington, Manager of Resource Services
		Distribution:	Vince Rimmington, Manager of Resource Services

1. EXECUTIVE SUMMARY

AUDIT CONCLUSIONS AND SUMMARY

We have carried out a high level review of key control areas within the control framework applied to the IT infrastructure and operating environment. The objective of our review was to assess the control framework and risks which may be present in order to provide the Manager of Resource Services with a structured plan for the detailed review of the IT and Information Security control framework for integration into the Internal Audit Strategic Plan.

In carrying out our review we have also identified some areas where we consider improvements would benefit the control framework. In respect of the seven areas of IT activity covered by this report, we have made a total of 24 recommendations, 7 of which we consider to be high risk issues. These have been discussed with the Manager of Resource Services, ICT Projects Team Manager, IT Services Technical Manager and the Head of Personnel & Organisational Development and we are informed that these areas will be addressed. Our findings are detailed in the accompanying report and action plan.

KEY ISSUES

Key issues identified with respect to the Council's IT systems, include:

- Business Continuity Plans, Initial Risk Assessments and Business Impact Analyses have not been completed;
- There is no up to date IT Disaster Recovery Plan in place;
- The server room presents unnecessary fire hazards;
- Windows service packs and hot fixes are not applied on a timely basis;
- Test servers are not available for all critical systems;
- Accounts with administrator access are not subject to regular review; and
- Data restore procedures are not formally documented and full restores of all servers are not carried out.

2. MANAGEMENT SUMMARY OF SUGGESTED ACTION

Rec.	Areas for Suggested Action	Risk Prioritisation	Management Comment
1.3	Business Continuity Plans should be finalised, and subject to regular testing and updates. Initial risk assessments should be completed for each business area and formally documented. Business impact reviews should be re-assessed and independently reviewed in light of the overall business continuity arrangements and needs of the Council. Alternative working and processing facilities should be established for the continuity of critical business systems.	High	Initial risk assessments have been completed for all Business areas. Workshops have been completed, in conjunction with consultants from Zurich Municipal, to identify and review priority services. Resource requirements have been identified, these will feed into the Disaster Recovery plan for critical business systems. The BCP is currently being updated to reflect the review activity undertaken. The plan will be subject to periodic review and a test programme will be developed and implemnted.
1.4	An IT Disaster Recovery Plan should be formally documented, approved, and distributed to all relevant personnel. Procedures should be tested on a regular basis.	High	Agreed. The Council has included this as a 2007/08 Key Task with a completion date of 31st March 2008. The task includes the establishment of a viable solution should a disaster occur. There is current Partnership activity in support of this objective.
2.1	The fire exit in the server room should be kept clear and accessible at all times. Any flammable materials and redundant equipment should be removed from the server room, and stored in an alternative location.	High	Agreed – may raise storage issues.
2.2	The Council should consider utilising Windows Server Update Services to quickly and reliably deploy the latest security and critical updates to their machines. Automated synchronisation should be set to search for updates on a daily basis.	High	Agreed in principle subject to Line of Business Application constraints. To be investigated
2.3	Test servers should be available for each critical system to ensure that adequate testing can be carried out prior to any system upgrades or enhancements to production systems, and for contingency in case of system failure.	High	The Council has 'test' environments for the primary line of business applications but in some instances they exist on the same platform. Agreed in principle but suggest that this may be achieved in the short term using a 'test rig' facility and that longer term the Council must engage in activity in support of Server consolidation.
3.3	Management should review accounts with administrator access on a regular basis, and remove any which are not required. In addition, the 'Administrator' account should be renamed.	High	Agreed.

4.2	Restore procedures should be formally documented and full restores of all servers should be carried out on a periodic basis.	High	Agreed
1.1	The Information Technology Security Policy should be reviewed and updated to include all areas of best practice recommendations. The policy should be formally approved and communicated to all staff.	Medium	Agreed
1.2	A review should be conducted to determine whether it is appropriate for the Manager of Resource Services to retain responsibility for business continuity planning and management.	Medium	Although independence of the Audit function is a key issue, in a relatively small organisation there is inevitably some minor conflicts of interest. The decision to locate the responsibility for co-ordinating Business Continuity across the Council within the Resource Services Section was done in knowledge of this potential conflict. It was considered that the best use of professional knowledge and the operational synergies of being located alongside Risk Management and Insurance Advice were in the best interests of the council.
2.4	Rules for allowing traffic through the firewall should be documented as part of the Council's information security policies and procedures. In addition, Change control procedures for amendments to the firewall rule settings should be introduced.	Medium	Agreed
2.7	The Council should obtain assurance from their Insurer that all necessary threats and perils are included within the policy for computer equipment.	Medium	It has been confirmed with the Authorities Insurers, Zurich Municipal, that such threats and perils to computer equipment is covered within insurance policy QLA10H0730113. The Authority completed a tender exercise for the renewal of its Insurance policy in March 2007. The criteria for submission of tenders included cover for all computer equipment.
3.2	Any accounts which are no longer required should be deleted or disabled.	Medium	Agreed
3.4	Issues raised in the vulnerability reports should be reviewed and resolved within reasonable timescales.	Medium	Agreed
3.5	Audit event logs should be monitored and reviewed, and any attempted violations or anomalous events actioned by management accordingly. Consideration should be given to enabling security event logs.	Medium	Agreed
4.1	The off-site location of backup tapes should be documented, and management should ensure that the security of the backup media is adequate.	Medium	Agreed

5.1	Data classification standards should be put in place to define the security level of data and how it should be handled.	Medium	Agreed – with particular regard to removal of data from site
5.2	The PC/Equipment Disposal procedure should be updated to reflect current practices. It should include responsibilities for the disposal and wiping of computer media and equipment, and all staff should be made aware of the procedures. Formal contractual arrangements should be put in place with the third party disposal company.	Medium	Agreed – need to investigate formal arrangements
6.2	Clear definitions for 'inappropriate material' should be agreed by senior management and clearly documented for all staff.	Medium	Agreed needs endorsement from SMT
6.3	Consideration should be given to configuring Mail Sweeper to scan and block messages with inappropriate content. The Council should clearly state their monitoring arrangements to all users.	Medium	Agreed but needs SMT input
7.1	The Data Protection Policy Statement should be approved as soon as possible, and communicated to all staff.	Medium	Agreed, will be submitted for approval and subsequently cascaded to staff.
2.5	Management should consider installing alternative power supplies for business critical applications.	Low	UPS are deployed for controlled shutdown of critical systems. If the Council were to suffer long-term power interruption would the D/R plan be activated?
2.6	A documented policy should be developed for the centralised acquisition of all hardware and software, and communicated to all relevant personnel.	Low	Agreed – some low value acquisitions are not centrally managed
3.1	Management should consider amending password settings in line with best practice recommendations.	Low	Agreed – may be dependant on facilities within some applications
6.1	The Employee Handbook should be updated to reflect the current policy on private use of Internet resources.	Low	Agreed

3. BACKGROUND, SCOPE and OBJECTIVES

We undertook an IT Health Check review during November 2006 at Gedling Borough Council as part of our internal audit plan for 2006/07. The health check identifies the areas that in our opinion would benefit from specialist IT audit review and therefore inclusion in the annual IA plan. It is necessary, however, for management to consider the results and make their own judgement on the risks affecting the Council and the level of specialist computer audit coverage they require in order to provide assurance that these risks are minimised. Our perceptions of the audit issues are based upon fact-finding interviews and observations made whilst on site during November 2006. In this regard and also in relation to any changes that may occur within the Council and within the technology employed, the areas for IT audit review subsequently referred to may need to be refined on an annual basis.

The objective of our review was to assess the following risks commonly associated with the IT control framework to determine the adequacy of internal controls, processes and procedures governing the IT control framework and operating environment and to identify areas of immediate significant risk.

- Loss of availability of systems;
- Loss of data;
- Inability to restore and recover;
- Inadequate IT performance;
- Unauthorised access;
- Inappropriate usage; and
- Failure to comply with legislative or regulatory requirements.

In order to satisfy the objective of the review the following areas were covered;

- Corporate policies and procedures are in place defining strategic direction and management of information security;
- Adequate precautions exist to protect the IT infrastructure and operating environment;
- Adequate precautions exist to ensure that data and software is well protected from loss, misuse, theft, damage and accidental or deliberate corruption;
- Arrangements exist for creating back-up copies of data and programs, storing and retaining them securely, and recovering applications in the event of failure;
- The transfer of data and IT facilities to and from the organisation is fully secure and third party access to IT facilities is fully protected;
- Use and control of the Internet and E-mail;
- Compliance arrangements for the Data Protection Act 1998.

From our review of the above, we have indicated those areas of risk for management to focus their attention upon and agreed recommendations with management where the potential exists to develop, enhance and strengthen procedures and controls.

Limitations to the scope of the review:

The scope of our work was limited to those areas examined and reported upon in section 4 in the context of the objectives set out above. We have carried out a high level review and this has only included compliance or substantive testing of the Council's systems, controls or data to the extent necessary for the purposes of gaining an overview of the control framework in place. It should not, therefore, be considered as a comprehensive review of all aspects of operational and infrastructure security or to detail all errors or risks that may currently or in the future exist within the IT environment, infrastructure or procedures of Gedling Borough Council.

With regard to the Data Protection Act 1998; compliance with the 1998 Act can be a complex issue and our review of this area for the purposes of this health check is limited to an overview of the strengths or weaknesses of the control framework in place.

Acknowledgement

We would like to record our appreciation to the staff of the organisation for the time and co-operation provided during our review.

4. FINDINGS

Control Objective 1:	Corporate policies and procedures are in place defining strategic direction and management of information security

In considering this, the need for the following best practice controls was considered:

- A suitable IT strategy detailing the IT development and direction for the Council.
- A properly documented and up to date IT Security Policy that assigns responsibility for IT security, covers all areas of best practice defined by ISO 17799:2005 and is properly communicated to all staff. Management procedures should be in place to monitor adherence to the policies, which should include the disciplinary action that may be taken for any breaches of the policy.
- A business impact review to establish the criticality of systems and key personnel, the nature of risk to which they are exposed and contingency measures to be implemented.
- Adequate training for users on Information Security and use of IT resources.

An IT Strategy is important in ensuring that the business objectives of the Council are adequately addressed by the development and provision of the IT infrastructure and applications.

The Council has developed an ICT Strategy which covers the period 2005 – 2008. This includes information on the current position of the Council, objectives, vision for the future, roles and responsibilities and an action plan. The Strategy document is to be reviewed on an annual basis alongside the normal end of year performance management arrangements.

The ICT Strategy was approved on 1 December 2005 by the Cabinet, and this is evidenced through the Cabinet minutes.

There is an Information Technology Security Policy which is on the Council's Intranet and is dated 27 April 2006. It includes sections on:

- Computer equipment (including portable devices);
- Computer software and data;
- Contracts, agreements and licenses;
- Access control;
- Password guidelines;
- Secured areas;
- Internet and e-mail access;
- Virus control;
- Removable media;
- Remote working policy; and
- Database development.

There is a separate section which gives an overview of the Data Protection Act 1998 and lists the 8 principles.

The Information Technology Security Policy was reviewed at high-level only; however, it was noted that although many of the areas of best practice as defined by ISO 17799:2005 are included, they are not in enough detail and some areas are not included at all, such as security incident procedures, network perimeter controls, software access, acquisition of computer equipment. In addition, it does not clearly assign responsibility for information security, and has not been formally approved by senior management to ensure acceptance of the policies and guidelines. Responsibility for regular review and update has not been defined.

The Information Security Policy is considered within ISO 17799 as a best practice control for the responsible control of information security, sets out management commitment to information security within the organisation, and provides clear direction on responsibilities and procedures. In addition, the adoption of an Information Security Policy now forms part of the mandatory security statement required to be completed by data controllers as part of the notification process under the Data Protection Act 1998. As such it should be clearly documented so that staff

are fully aware of their responsibilities and the Council's policies and procedures.

Recommendation 1.1
The Information Technology Security Policy should be reviewed and updated to include all areas of best practice recommendations. The policy should be formally approved and communicated to all staff.

The Manager of Resource Services, who is also head of Internal Audit, has overall responsibility for Business Continuity. Such close involvement in this crucial business process may compromise the independence and objectivity required by the audit function.

Recommendation 1.2
A review should be conducted to determine whether it is appropriate for the Manager of Resource Services to retain responsibility for business continuity planning and management.

There is a project underway to update and document Business Continuity Plans, and workshops are being carried out across the business to populate a template document. This process is due for completion by December 2006, when it will be tested using a number of scenarios. The Plans will then be subject to annual review and update.

Each department is responsible for generating their own departmental Business Continuity Plans, and initial risk assessments have been completed. However, on review of a sample of completed risk assessment documents, it was noted that these are actually questionnaires to determine resource requirements and what plans and procedures are in place. One of the questions asks, "Have you assessed the risks associated with each key function and identified any necessary control measures?" Five were selected at random (Personnel & Service Development, Housing Services, Environmental Protection, Planning & Environment and Direct Services) and all had answered 'no' to this question.

In addition, 'Key Functions by Time Frame' documents have been completed by each business area to consider all of its key processes and assess how long they can sensibly operate without that process being performed. It was noted that there was a great deal of variance in the way the forms had been completed. For example, Leisure: Community Centres have determined that all of their key processes must be operational within 24 hours. These functions include room hire, cleaning of buildings and car parking. In contrast, Planning and Environment: Food/licensing/Health & Safety can operate for up to 3 months without any of their key processes. These assessments need to be reviewed independently and considered in light of the overall continuity of the Council's business processes – it is unlikely that cleaning buildings and room hire would then be categorised as the highest priority.

Recommendation 1.3
The following recommendations have been made in respect of Business Continuity Planning and Management: • Business Continuity Plans should be finalised, and subject to regular testing and update. • Initial risk assessments should be completed for each business area and formally documented. • Business impact reviews should be re-assessed and independently reviewed in light of the overall business continuity arrangements and needs of the Council. • Alternative working and processing facilities should be established for the continuity of critical business systems.

There is currently no formally documented IT Disaster Recovery Plan. Until June 2006 there was a contract in

place for disaster recovery arrangements, but as this has now ended, there is no provision in place. A spreadsheet was produced in November 2005 listing the servers and applications in use by the Council, and scores were awarded by the ICT Strategy Group according to their criticality. Ratings from 1 to 4 determine how quickly they need to be recovered in the event of a disaster (recovery factor 1 was 1 week; recovery factor 4 was 4 weeks).

Standby facilities in the event of a disaster have not yet been established; in the event of a disaster all computer equipment will need to be purchased and installed separately. A proposal was sent to the Senior Management teams at Gedling Borough Council, Mansfield District Council and Broxtowe Borough Council in September 2006 to form a partnership arrangement in providing each other with designated space and equipment to enable the continuity of critical business processing following a disaster event. This is currently being considered by each party.

In the event of a disaster resulting in partial or total loss of critical computer equipment, key IT systems may not be recovered within reasonable timescales resulting in systems unavailability and disruption of business processes.

Recommendation 1.4
An IT Disaster Recovery Plan should be formally documented, approved, and distributed to all relevant personnel. Procedures should be tested on a regular basis.

There is an induction course run for all new starters which includes an introduction to IT systems and basic training on information security and the use of IT resources. Responsibilities in relation to the Data Protection Act 1998 are outlined, and the Information Technology Security Policy is covered. In addition, guidelines on virus protection and reporting, business recovery, shutting down/logging off the network and internet and e-mail access are included.

In addition, a user guide on the use of networked PCs has been developed, which includes basic training notes on Microsoft products, troubleshooting, saving and retrieving files, virus scanning, printing and logging on and off.

Control Objective 2:	Adequate precautions exist to protect the IT infrastructure, operating environment and the resources they support.

In considering this, the need for the following best practice controls was considered:

- Hardware and Communication media should be protected against damage, malfunction and misuse. Suitability of locations and the ability to restrict access should be given due consideration. The critical computer equipment is protected against environmental risks. There are no obvious environmental hazards in, over or surrounding the immediate vicinity of critical resources.
- A procedure is in place to ensure that critical operating system service packs and security hot fixes are applied on a timely basis. All known security packs and hot fixes have been assessed and applied where considered appropriate.
- Rules for allowing traffic through the firewall have been documented as part of the Council's information security policies and procedures.
- There is adequate resilience built into servers and network routing. Alternative power supplies should be installed where business-critical applications are processed. Performance monitoring and support contracts minimise risk of failure and excessive downtime. All failures are recorded by management. An adequate support contract is in place.
- All items of computer equipment and software should be recorded in inventories for the purpose which records make, model, version, serial number / licence number, cost, date of purchase and invoice number.
- Adequate arrangements exist to ensure insurance cover is in place for computer equipment. The policy should include coverage for all risks including fire and flood damage, theft and vandalism. The cost of additional processing in the event of loss along with that to reconstitute data should also be included.

The Council's critical hardware and communication media is located within the server room which is located in the ICT department on the first floor of the Civic Centre building.
Access to the server room is secured via a key pad code which is known by ICT Support staff only. We understand that when staff are present within the ICT department, the door is left unlocked. The server room can only be accessed through the ICT department; access to which is further restricted via two doors with separate access codes.
The caretaker also has a key to the room in case ICT staff are unavailable to deal with any incidents outside of working hours.

The server room has an HFC 227ea gas-drop fire suppression system installed. It was noted that the canisters had last been serviced on 20 September 2006. In addition there is a CO^2 fire extinguisher which was last serviced on 16 December 2005. All new staff are trained in the use of fire-fighting equipment, and alerted to the dangers of the fire suppression system and safety procedures.

There are two Denco air conditioning units which run independently from each other and can support the whole room in case of unit failure. One was reading at 21.9 degrees and the other at 22.2 degrees. In case of failure, there is an alarm system within the ICT department which is activated; no out of hours support is in place.

Under floor water detectors are in place which are also alarmed. There are three smoke detectors in the server room which are tested on a regular basis.

There are no windows in the server room, but there are two doors. One is the main door which is locked out of hours, and the other is a fire door leading to the Council Tax department. Access can only be gained from inside the server room; testing revealed that entry cannot be gained from inside the Council Tax department. However, at the time of the audit, the door was being obstructed from within the Council Tax department; as this is a fire door, access should remain clear at all times to enable safe and speedy exit in case of a fire.

We noted that spare computer equipment, media and boxes are stored in the server room, as alternative storage

facilities are not available. Flammable materials and redundant equipment stored in the server room may increase the risk of fire damage.

Recommendation 2.1
The fire exit in the server room should remain clear at all times. Any flammable materials and redundant equipment should be removed from the server room, and stored in an alternative location.

There is no procedure in place to ensure that critical operating system service packs and security hot fixes are applied on a timely basis. Service Packs are installed onto servers following recommendations by the software vendor; hot fixes are not applied to client machines.
The Council has considered installing Windows Server Update Services (WSUS), although this has not been taken forward.
Testing is not always carried out prior to upgrades, as for many of the applications there are no additional test servers.

Unless critical operating system service packs and security hot fixes are applied on a timely basis, the Council's systems could be vulnerable to security weaknesses and system bugs. Testing should be carried out prior to any system upgrades or enhancements to identify any detrimental implications prior to live installation.

Recommendation 2.2
The Council should consider utilising Windows Server Update Services to quickly and reliably deploy the latest security and critical updates to their machines. Synchronisation should be set to search for updates on a daily basis.

Recommendation 2.3
Test servers should be available for each critical system to ensure that adequate testing can be carried out prior to any system upgrades or enhancements, and for contingency in case of system failure.

The Council has installed Symantec Enterprise Firewall 8 as their firewall solution.

Rules for allowing traffic through the firewall have not been documented. Unless firewall rule settings are documented, re-configuration may not be possible within a reasonable timescale, and in the event of a change in personnel, the reasons for rule settings may not be clear resulting in unnecessary or inappropriate changes.

We understand that only two members of the ICT team have access to make changes to the firewall rule base settings; however, there is no change control procedure in place. Firewall rule changes should be authorised appropriately and justifications documented; otherwise unauthorised or inappropriate changes could result in loss of service or security vulnerabilities.

Recommendation 2.4
Rules for allowing traffic through the firewall should be documented as part of the Council's information security policies and procedures. Change control procedures for amendments to the firewall rule settings should be introduced.

An Uninterruptible Power Supply (UPS) is in place for all critical systems, providing enough time to safely shut down the systems in the event of power loss. There are no alternative power supplies in place.

GFI Network Server Monitor is being utilised by the Council for performance monitoring. It monitors and reports on issues such as disk space, web proxies, it can ping network devices, and notify if PC Anywhere is left running. The system has been configured to send an email notification to the IT Support team in the event of non-compliance with pre-defined parameters.

Event Reporter by Adiscon is used to filter and report on key events (errors and warnings), and e-mail

notifications are sent to IT Support for review and action.

Recommendation 2.5
Management should consider installing alternative power supplies for business critical applications.

A record of all hardware and software assets is maintained through the SunRise helpdesk system. This includes an asset tag, manufacturer, model number, serial number, IP address, supplier, cost, etc.

To ensure that IT are aware of all new purchases of IT equipment and software, and any disposals, there is a centralised acquisition policy, although this has not been documented. All hardware is assigned a unique identification number, and IT staff enter the details onto the system. Any specialist software which is installed locally on workstations is linked to the unique identifier to enable the monitoring of software against licenses held.

Unless staff are aware of the centralised acquisition policy, there is a risk that hardware and/or software is purchased by individuals or departmental areas, resulting in increased costs, inaccurate inventories and potential software licensing issues.

Recommendation 2.6
A documented policy should be developed for the centralised acquisition of all hardware and software, and communicated to all relevant personnel.

The Council has a current insurance policy with Zurich Municipal which is due for renewal on 30 March 2007. The cover includes material damage to computer suite equipment whilst on the premises and other computer equipment whilst in the territorial limits. However, the only perils insured relate to accident and breakdown where not covered under maintenance services. Fire perils, theft and vandalism are not included within the computer equipment policy; although we understand that this is covered at corporate level as claims have been made previously.

The insurance policy and sum insured is reviewed annually, and confirmation is obtained from IT that the level of insurance cover for computer equipment and additional processing costs remains adequate; based on the values within the asset inventory.

Recommendation 2.7
The Council should obtain assurance from their Insurer that all necessary threats and perils are included within the policy for computer equipment.

Control Objective 3:	Adequate precautions exist to ensure that data and software is well protected from loss, misuse, theft, damage and accidental or deliberate corruption.

In considering this the following points were discussed:

- Procedures should exist for the application and authorisation of user accounts and the control of access to information. A suitable logical security framework should be in place for the effective setting of domain and user account settings. Password syntax should reflect the security level of the user.
- The number of copies of a software package are reasonable for the number of users, and costs minimised by standardising on a single package. Advantage is taken of site or multi-user licenses, or installing multi user software on PC servers to reduce the cost of installing standalone copies of software on all PCs.
- Suitable and current anti virus software is installed on equipment. Adequate procedures should exist for its regular update and installation. Controls should be in place to minimise the risk of virus infection from external sources.
- Intrusion Detection controls are in place to detect other types of malicious software not detected by anti-virus controls.
- Adequate monitoring procedures should be in place to ensure that security has not been breached. Systems and Audit event logs are enabled, appropriately set and monitored. Attempted violations or anomalous events are reported to and actioned by management.
- Controls ensure that confidential output should be disposed of securely.

Prior to being granted with access to the Council's networked resources or applications, an IT Access Form must be completed by the individual's supervisor to request access to systems in line with their job role and responsibilities. This form is signed by the supervisor and retained by the Senior Computer Operators.

The new user must sign to agree to abide by the Internet and Email guidance notes, but not the Information Technology Security Policy or supporting procedures.

A sample of 12 users was selected at random to determine whether appropriately authorised forms had been completed and retained. Ten forms had been retained; only six had been signed by the user as accepting the internet and email policy. One form had not been retained, as the user had joined the Council before the forms were introduced. One new starter had been set up with network access (and the account was enabled) before they had started, and consequently had not completed an access form. Another user had joined the Council in August 2006, and been set up with network access; however, the completed form had still not been received by their line manager giving authorisation.

To determine whether user access is appropriate and users are being removed from the system within a reasonable timescale, accounts were extracted where the user had never logged on, or had not logged on for over 30 days, and the account was still active. This revealed 249 accounts (there is a total of 670 users, including service accounts).

Redundant accounts are a potential target for hackers as use of the account could go unnoticed. Unless review of these accounts is carried out, there is no assurance that these accounts are appropriate.

A list of staff who have left the Council since September 2006 was obtained, and testing was carried out to determine whether their network access had been removed. 13 out of 14 accounts had been deleted; one had the password reset, but the account was still active. Leavers' accounts should be deleted or disabled to prevent unauthorised access.

Data extracted from the domain revealed that the following domain policy settings have been applied:

- Minimum Password Length = 6 Characters;
- Max Password Age = 60 days, best practice recommends 30 days;

- Minimum Password Age = 0 days, ideally this should be set to at least 1;
- Password History = 12 passwords;
- Reset bad logon count after 30 minutes;
- Lockout duration = 30 minutes, ideally accounts should be locked out until unlocked by an Administrator;
- Lockout after 5 bad logon attempts, best practice recommends 3 failed attempts.

Best practice for password use is defined within BS ISO/IEC 17799 Information Technology – Code of Practice for Information

Security Management. Although most of the settings conform to best practice recommendations, the Council should consider amending the password age and account lockout settings.

Testing revealed 24 accounts within the 'domain admins' group; these were examined for appropriateness. Ten of these accounts are either no longer required, or do not require domain admins access. Regular review of domain admins users would reduce the risk of redundant accounts or inappropriate access.

It was noted that the administrator account has not been renamed. Due to the high level of privileges afforded this account, it is a potential target for hackers, and must be kept secure.

Recommendation 3.1
Management should consider amending password settings in line with best practice recommendations.
Recommendation 3.2
Any accounts which are no longer required should be deleted or disabled.
Recommendation 3.3
Management should review accounts with administrator access on a regular basis, and remove any which are not required. In addition, the 'Administrator' account should be renamed.

The Council has installed Sophos as their anti-virus solution for all clients and servers. Sophos Enterprise Manager is used to automatically update when new definitions become available. Synchronisation is set to search for updates on an hourly basis, seven days a week.

A sample of five servers were selected and tested to verify that the latest virus definitions had been applied. All servers had the virus definition 4.11 installed. The Sophos website confirmed that this was the latest version available.

Vulnerability testing is carried out on a regular basis; the most recent report produced by NTA Monitor Ltd is dated May 2006. This highlights security issues, of which there were 2 of medium severity, 7 of low severity and 3 for information. The report states that none of the issues have been fixed since the last report, and only 1 issue was new. Therefore 8 issues had been raised previously but not addressed (excluding the 'information' issues).

The Council should be proactive in resolving security issues raised, to improve the resilience of the network and protect it from security vulnerabilities.

Recommendation 3.4
Issues raised in the vulnerability reports should be reviewed and resolved within reasonable timescales.

Application and system audit event logs are produced, but are not proactively reviewed. Security event logs are not enabled.

Without formalised processes for reviewing event logs, security incidents or system misuse could go undetected, and system failures may not be resolved in a timely manner.

Recommendation 3.5
Audit event logs should be monitored and reviewed, and any attempted violations or anomalous events actioned by management accordingly. Consideration should be given to enabling security event logs.

Within each department there is a recycling bin for the disposal of non-confidential information. In addition, there is a plastic box for confidential waste in each office; administration staff collect this on a periodic basis for shredding. Some offices have their own shredders.

Control Objective 4:	Arrangements exist for creating back-up copies of data and programs, storing and retaining them securely, and recovering applications in the event of failure

In considering this the following points were discussed:

- Data and programs are subject to a documented backup regime, including security of backup media, restore testing and change control.
- Documented procedures should clearly state the process to follow should systems fail or a contingency event occur. Periodic full restore tests are carried out to ensure that backup media and recovery procedures are sound and reliable.

Detailed backup procedures have been documented which include backup cycles, on-site location of tapes, frequency of taking tapes off-site (although the location has not been specified), ARCServe and Veritas backup logs, tape formatting, and checking error reports.

Backup tapes are stored within two fireproof safes at the Civic Centre. The keys to the safes are retained in the Computer Room, and a spare set is retained off-site at the home of the Technical Manager.

We understand that backup tapes are taken off-site every week and stored in a fireproof safe at the Richard Herrod Leisure Centre [this was not verified during the review]. This is just over 3 miles away from the Civic Centre.

A sample of backup schedules was extracted from the Veritas Backup Exec and Arcserve systems, which verified that full backups are being taken on a daily basis.

Recommendation 4.1
The off-site location of backup tapes should be documented, and management should ensure that the security of the backup media is adequate.

At present, scheduled restore testing is not carried out; however we understand that regular data restores are carried out, usually of data files accidentally deleted by users, and database restores. There are no formally documented restore procedures detailing the process to follow should systems fail or a contingency event occurs.

Without carrying out scheduled full system restores, the Council cannot be assured as to the integrity of the backup media or that systems can be fully recovered using the backup disks in the event of a failure.

Recommendation 4.2
Restore procedures should be formally documented and full restores of all servers should be carried out on a periodic basis.

Control Objective 5:	The transfer of data and IT facilities to and from the organisation is fully secure and third party access to IT facilities is fully protected.

In considering this the following points were discussed:

- Adequate classification standards are in place, which defines the security level of data and how it should be handled. Control mechanisms are applied to reduce the risk of unauthorised disclosure of confidential or sensitive data and loss of data integrity.
- Any data and equipment for disposal does not contain information which should not be disclosed and procedures exist for the secure wiping of all HDD prior to disposal of obsolete or transferred kit.
- Appropriate access control mechanisms are in place for remote access to the Council's resources, such as RAS server dial back, and challenge response authentication. The risks of third party connections have been fully evaluated and security procedures are reflected in a written contract.

Although there are not currently any data classification standards in place for the handling and transmitting of sensitive, personal and business confidential information, we understand that these are being considered in conjunction with the ESD (Electronic Service delivery) Toolkit and Government Connect. Each interaction is being reviewed, such as booking services, paying bills, applying for licenses, etc. with a view to determining their level of classification.

It is important that the classification informs staff of how and where the different data classes can be stored, such as on laptops, which classes may be transmitted or used in e-mails, and whether encryption is to be used. It is also suggested that as part of loaning laptops to staff, data storage and processing of sensitive information is highlighted within an agreement which staff are required to sign up to.

Recommendation 5.1
Data classification standards should be put in place to define the security level of data and how it should be handled.

The PC/Equipment Disposal procedure was reviewed and it was noted that responsibility for the disposal and wiping of hard disk drives has not been defined. Although the ICT department has a shredder for the disposal of compact disks (CDs), users are not made aware of this through the disposal policy, and may seek to dispose of media through another, less secure method.

There is a five-year replacement programme for all desktop equipment, and data is wiped from the machines prior to disposal. The disposal procedure states that this is done via format and fdisk, although we understand that it is actually done using the freeware product 'Adrik's Boot and Nuke' which uses the US Department of Defence 5220-22.M. Equipment is then sent to RDC (which forms part of Computacenter (UK) Ltd) who are responsible for ensuring all data is permanently removed, and components are recycled where possible, or disposed of in an environmentally friendly way. Compliance statements are produced by RDC after each disposal which state, "All data bearing media will have protected data eradicated using proven and certified processes or the media will be disabled before recycling – no protected data is released, in accordance with the Data Protection Act 1998". However, there is no formal contract with RDC. The signatures on the disposal schedule relate to overseeing the collection, and not the compliance statement. Therefore it may be difficult to prove liability in the case of a dispute or unlawful disclosure of data.

In addition, the process for the safe and secure wiping of media is not documented.

The Seventh Principle of the Data Protection Act 1998 states that, 'Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.' Unless responsibilities and procedures for the secure and safe disposal of data and equipment are clearly defined and documented, and contractual arrangements are in

place, this may result in the unlawful disclosure of personal or sensitive information.

Recommendation 5.2
The PC/Equipment Disposal procedure should be updated to reflect current practices. It should include responsibilities for the disposal and wiping of computer media and equipment, and all staff should be made aware of the procedures. Formal contractual arrangements should be put in place with the third party disposal company.

Remote access to the Council's networked resources is available to all staff to enable an effective means of communication for home-working purposes and remote users such as visiting inspectors and planning regulators. Access to the network is via a Virtual Private Network (VPN), and users authenticate using user ID and passwords.

A Home-Working policy has been documented. It includes as an appendix an operational agreement which includes a clause on security and confidentiality.

Third party suppliers occasionally need remote access for diagnostics and fault fixes; this is granted via a VPN connection. In these cases, a change control form is completed to authorise the dial-in request and record the date and time of access, time of dial-in termination, and which systems were accessed. If there was a need to monitor access, logs could quickly and easily be produced from the details recorded on these forms.

Control Objective 6:	Use and Control of the Internet and E-mail.

In considering this the following points were discussed:

- E-mail and internet acceptable use policy has been documented and adequately communicated, setting out a practical framework for staff whilst ensuring the confidentiality, availability and integrity of the organisation's network and computer systems.
- The internet is behind a suitable firewall.
- Content scanning/blocking software is in use. Monitoring for abuse/unacceptable sites is possible from log information and carried out. E-mail spam controls are in place such as the use of message labs to filter pre-agreed potential unacceptable content. The release of quarantined mail to the user is adequately controlled. A sample of the Internet usage for a predetermined period can be analysed if required to provide Management with a view on the compliance or otherwise with the Organisations acceptable use policy.

Within the Information Technology Security Policy, section 2.3.8 provides a cross reference to the Employee Handbook for the acceptable usage policy for Internet and Email resources.

Guidance notes on use of Internet and E-mail facilities are included within the Employee Handbook (Appendix 4). The introduction explains the purpose of the resources, potential risks of abuse, the need to comply with legislation, and the consequences for non-compliance.

The notes state that the facilities can be used for personal use, but not within core hours or work time. Permission must be obtained from line management prior to personal use, and any time should be recorded and paid for. However, in the SMT Briefing dated 23 May 2006, it was agreed that charges for private Internet usage will no longer be applied.

Additional information includes:

- Programs and utilities must not be downloaded without IT consent;
- Monitoring of usage will be carried out by the IT department;
- Virus control;
- Access to inappropriate sites;
- Harassment;
- Circulation of file attachments.

The Guidance Notes state that users should inform the IT department if 'inappropriate material' is accessed. However, it does not clearly state whether accessing 'inappropriate material' would result in disciplinary action. 'Inappropriate material' includes material which is illegal, pornographic, racist, sexist or offensive, and although it states that the list is not exhaustive, in order to ensure compliance and improve clarity, the Council should consider including categories such as chat, dating, games, hacking, violence, and weapons. It should remain consistent with the categories configured within WebSweeper.
In addition, in relation to e-mails, the Guidance Notes should include contractual obligations, copyright, sending personal data via e-mail (to comply with Data Protection regulations), virus threats (i.e. not opening attachments from unknown sources), and housekeeping (the need to regularly delete emails to prevent overloading the system, and to comply with Data Protection Act 1998 if they contain personal data).

Unless acceptable usage is clearly defined, monitoring compliance with the policy and applying disciplinary action may become difficult.

Recommendation 6.1
The Employee Handbook should be updated to reflect the current policy on private use of Internet resources.

Recommendation 6.2
Clear definitions for 'inappropriate material' should be agreed by senior management and clearly documented for all staff.

The Council has installed Symantec Enterprise Firewall 8 as their firewall solution.

The firewall is situated between the Internet and the internal network.

WebSweeper is used to filter and block unacceptable websites. The rules list was examined to determine which categories have been blocked; this includes chat, gambling, games, glamour & intimate apparel, and personals & dating.

Categories such as adult/sexually explicit material, criminal skills, hacking, hate, personal websites, remote proxies, violence and weapons, have been set as 'alerted'. In addition to blocking the website, an alert is also sent via e-mail which is checked by the Senior Technical Officer. If it is deemed to be a deliberate attempt to violate the policy, it is reported to the Technical Manager; it would then be passed to the appropriate line manager to deal with, and if necessary proceed to the corporate disciplinary procedure.

If line managers suspect inappropriate or excessive usage, reports are generated for review. In addition, monthly reports are generated on the top ten users and top ten websites accessed. These are reviewed by the Head of Personnel & Organisational Development to identify any policy breaches for disciplinary action.

The Council utilises Softscan to initially scan and block unwanted e-mail messages; any containing viruses or spam (matching word for word) are automatically dropped. Any which are borderline spam are quarantined for review by the IT Services team, and either released or dropped. Legitimate emails then progress to the Council where MailSweeper is used to perform second level checking. Although MailSweeper can be configured to include the scanning and blocking of profanity words, this has not been applied. This could result in reputational damage to the Council.

Recommendation 6.3
Consideration should be given to configuring Mail Sweeper to scan and block messages with inappropriate content. The Council should clearly state their monitoring arrangements to all users.

Control Objective 7:	Compliance arrangements for the Data Protection Act 1998

In considering this the following points were discussed:

- The Council has appointed a Data Controller.
- There is an adequate Data Protection Policy that informs staff of the Eight Principles.
- The Council has a current notification/registration.
- The Council has a procedure for dealing with Subject Access.
- All users have received adequate training on the Data Protection Act and their responsibilities towards personal information.

The Council has assigned the Senior Solicitor as the Data Protection Co-ordinator.

The Data Protection Policy has recently been updated and is due to go to the Cabinet for approval at the next meeting.

The Policy was reviewed at high-level, and was found to be comprehensive: it includes details on the 8 principles, responsibilities, contact details for the Data Co-ordinator, data disclosure, retention, security of data and subject access requests.

Recommendation 7.1
The Data Protection Policy Statement should be approved as soon as possible, and communicated to all staff.

Gedling Borough Council has a current notification Z7097798 which is due to expire on 10 October 2007. The Electoral Registration Officer of Gedling Borough Council has a current notification Z7660945 which is due to expire on 20 February 2007.

There are 13 purposes within the main Gedling notification.

The procedure for dealing with Subject Access requests is included within the Data Protection Policy Statement. It explains the process, timescales for responding, fees, and who the request should be forwarded to.

There is a 'Data Subject Access Application Form' for individuals to complete in order to obtain the necessary information and determine the types of data they are requesting.

Training sessions are held regularly for staff on the Data Protection Act 1998. Training evaluation forms are completed after the course to confirm understanding and identify any further training needs.

5. ASSESSMENT OF IT AUDIT REQUIREMENTS

The Internal Audit Department is responsible for carrying out an agreed programme of internal audit reviews, as detailed in the annual and strategic audit plans. The suggested IT audit plan shown at Appendix A will form part of the overall strategic plan for the Council. It is not possible, nor considered necessary, to cover all the Council's activities on an annual basis, but it is expected to cover all significant control areas within a rolling three year strategic plan. The frequency and timing of the reviews is primarily determined by an audit needs assessment exercise that is carried out on an annual basis.

The domain for IT audit coverage is the complete population of IT audit areas for which internal controls may be effectively and efficiently applied to reduce the risk. It is therefore likely to encompass all areas of activity of Gedling Borough Council.

The audit areas identified within the domain of audit coverage include:

- Any IT systems which support the operational processes of the Council;
- IT organisation and management;
- Organisational IT strategy and policies;
- The development and project management methodology applied;
- Specific IT projects within the Council;
- IT environments, including hardware, operating systems, networks, software
- Business application systems and Internet based systems;

In addition to the areas of specific IT audit coverage, IT audit work will include:

- Planning and co-ordination with the Manager of Resource Services;
- Supporting the work of the Internal Audit Department as may be requested from time to time, principally through the use of Computer Assisted Audit Techniques (CAATs), for data interrogation and validation, technical audit tools and vulnerability scanning software;
- Follow up of action taken by management to address previous recommendations;
- Ad-hoc special projects as requested where specific IT audit skills are required.

From the review observations it is our opinion that the IT Audit areas set out in Appendix A below would provide management with a level of assurance for the control of risk within the IT systems, infrastructure and operational applications employed.

As a general rule the usual starting point is an Installation Review, sometimes referred to as a Review of General Controls. The areas covered in this review would include those controls that have an overall impact on the computing environment and are not necessarily confined to a single IT area. However, it may be more beneficial for the Council to concentrate directly on the more immediate issues highlighted by the health check as it is these that expose the Council to the maximum risk. We have therefore based our plan in Table A on addressing the areas of greatest risk in the initial part of our plan.

APPENDIX A - SUGGESTED IT AUDIT PLAN 2007 – 2009

Audit Coverage – Information Security Audits	2007–08 Proposed audit days	2008 – 09 Proposed audit days
Business continuity planning (inc IT Disaster Recovery)	7	
Use and Control of the Internet and e-mail		7
Network Security (Windows 2000/2003 server security)	8	
Remote Access / Firewall Security Review		
Data Protection Act 1998 and Freedom of Information Act 2000		4
Application Security Reviews		
ICT security policy and procedures, including, information governance, security administration and induction training.	6	
ICT strategy and planning		
Systems Development and Change management		6
Segregation of duties and knowledge management– DBA arrangements		
Network Security Infrastructure and Environmental Controls		6
IT procurement and IT Inventory		
Risk assessment, Management and follow up	3	3
Total IS Audit Days	24	26