GEDLING BOROUGH COUNCIL

**FINANCE DEPARTMENT**

# RESOURCE SERVICES

# AUDIT REPORT

| | |
|---|---|
| TO: | J. Brothwell - Head of Personnel and Organisational Development<br>M. Lane - IT Projects Manager<br>G. Bennett - IT Technical Manager<br>M. Kimberley - Head of Finance<br>D. Kenworthy - Audit Commission |
| FROM: | V. Rimmington - Manager of Resource Services |
| AUDIT: | **IT AUDIT – Access Controls 2005/06** |
| DATE: | 12th September 2006 |

Attached is a copy of the **FINAL** Audit report with respect to the above review.

The report and its recommendations have been approved by the Head of Finance [section 151 Officer].

The comments received by you have been incorporated within the report. Should there be any changes or additional comments that you wish to inform me of, please do not hesitate to contact me.

In accordance with agreed procedures, a member of the audit team will carry out a follow-up review on the implementation of the recommendations made within the report.

Thank you for your assistance in this matter.

*Vince Rimmington*

**Manager of Resource Services**

# INTERNAL AUDIT REPORT

## COMPUTER AUDIT

## ACCESS CONTROLS

## C O N T E N T S

## 1. INTRODUCTION

1.1 The purpose of this audit assignment is to review **the Access Controls within the Authority and specifically within the IT environment** to, ensure that any logs / records maintained and supporting documentation conform to the Authority's IT policy and relevant legal and regulatory requirements. This is in accordance with the 2005/06 Audit Plan.

SCOPE AND COVERAGE

1.2. The audit review is the first in a schedule of planned IT audits and will review briefly the policy and the access control documentation together with access reports as reviewed by the managers.

1.3. Any findings, conclusions and recommendations will be discussed with Officers and members of staff before being included in a formal report or memorandum. It is intended to inform management of any findings on an ongoing basis and this will form the basis of a draft report/memorandum to the Head of Finance.

SYSTEM OBJECTIVE

1.4. System objective specified and assigned for this audit:

- Access to Program Documentation.
- Access to Systems Software.
- Access to Production Programs.
- Access to Data Files
- Access to On-Line Systems
- Access to Data Bases
- Password Administration
- Policies for Access Security

## 2. CONDUCT OF AUDIT

2.1 The audit scope and system objectives, outlined above, were followed and references were made to the IT user guide.

2.2 Discussions were held with the IT Projects and Technical Managers and Computer senior operators to establish the access controls and procedures followed by IT staff.

2.3 System notes were prepared from the discussions and the IT user guide obtained from the intranet.

2.4 A review of access controls was undertaken, and testing completed to assess compliance and provide assurance that controls are operating effectively. A number of recently purchased applications, including Agresso and Valid, are in the process of being implemented, therefore no detail review was undertaken on these applications.

2.5 The assistance and co-operation of all staff involved in this audit assignment is acknowledged and appreciated.

## 3. EXECUTIVE SUMMARY

3.1. The Majority of access controls identified during the audit assignment are operating effectively. However, there were weaknesses identified and the recommendations are summarised below. Staff members are experienced and knowledgeable and systems could be improved by ensuring that management review and monitor access to IT systems.

3.2. Access to individual systems will be reviewed during specific audits of the key financial systems and consider the controls that the system owners apply and monitor for all users.

3.3. Security within the IT environment is adequate, however full access to all systems is available to IT support staff, which is a requirement of their roles. There is no monitoring or review of IT support staff access which raises a potential risk for fraud or misuse.

3.4. The audit highlighted some control weaknesses that are considered to be of **Low to Medium** risk and are included in this report together with the recommendations.

## 3.5 CONCLUSION

Overall the security and access controls in place for IT systems are satisfactory. The new systems currently being implemented should mitigate the risks emanating from the recommendations made in this report.

## AUDIT ASSURANCE

As a result of the work undertaken during the audit, it is concluded that the IT access control arrangements in place are well controlled and the majority of controls are sound and operate effectively.

# ACTION PLAN

| REC (Risk) | RECOMMENDATION | RESPONSIBLE OFFICER | MANAGEMENT COMMENT | IMPLEMENTATION DATE |
|---|---|---|---|---|
| 4.2.4 **Low** | To safe guard data items [tapes/discs] locked in the fireproof safe, a log should be maintained of staff access. Alternatively all sensitive data items should be verified annually to ensure security. | IT Technical Manager | An annual audit of data will be undertaken to unsure the security of Gedling data. | By 31/3/07 |
| 4.4.4. **Low** | Consideration should be given by management to establishing a formal reporting/monitoring process of access attempts by users to the windows domain. | IT Technical Manager | We will set up a system to monitor account lock-outs via the helpdesk. This will record occurrences and look for patterns that require further investigation. | By 31/3/07 |
| 4.5.3. **Med** | Access forms should be available for all current users and most recent users to verify the access authorisation within the IT system. | IT Technical Manager | Forms have been reorganised to keep all of a users forms together as per discussions with Suresh Mistry. | 02/05/06 |