Internal Audit Report

CHIEF EXECUTIVE'S UNIT,
STRATEGIC FINANCE

GENERAL LEDGER

JANUARY 2013

1 INTRODUCTION

This report has been prepared as a result of the Internal Audit review of General Ledger controls and procedures maintained by Strategic Finance, Chief Executives Unit. The audit forms part of the 2012/2013 Internal Audit Planned programme of audits.

A review of specific aspects of General Ledger Operations is undertaken each year by Internal Audit as part of the annual audit plan. Last year's audit concentrated on entries to the financial management system.

General Ledger transaction values for 2011/12 obtained from a trial balance run are summarised below:

Four Main Council Bank Accounts	Totals £ 2011/02 DR	Totals £ 2011/12 CR
Income	449.9m	449.8m
Local Tax	67.6m	67.5m
Expenditure (Creditors and Payroll)	366.0m	364.3m
Housing Benefits	22.8m	22.8m
Total	**906.3m**	**904.4m**

As part of our ongoing dialogue and work co-operation with Audit Scotland, and to minimise audit interference in daily operations, the audit of the General Ledger was discussed with Audit Scotland and included agreed test sampling in key areas.

2 AUDIT SCOPE AND OBJECTIVES

Internal Audit has undertaken both a high level review and sample testing of the General Ledger to ensure the integrity and security of information input to and held on the General Ledger is robust and controlled. The areas reviewed included:

- Access to and operation of the General Ledger system;
- Authorisation of changes to the Chart of Accounts;
- Data from Feeder Systems is authorised, complete, valid and timely;
- Amendments by journals are authorised, complete, accurate and valid;
- Outputs are complete, accurate, appropriate and timely; and
- Data is protected against loss, corruption or system failure

3 RISK ASSESSMENT

As part of the audit process and in conjunction with our CIPFA Systems Based Audit (SBA), ICQ approach, the risk register was reviewed to identify any areas that needed to be included within the audit. The area identified was:

- SR16 Failure to have a robust internal control process and system

This risk has been considered within the scope of our audit.

4 CORPORATE GOVERNANCE

There were no Corporate Governance issues to be reported as a result of this audit.

5MAIN FINDINGS

5.1Access to the General Ledger system is restricted to appropriately approved members of staff with individuals granted different levels of access rights based on their specific job descriptions and user requirements. System reports of staff with user access rights are reviewed to confirm their continued requirements on a regular basis.

5.2 General Ledger procedures are documented and Oracle General Ledger User Manuals are widely available although there is no up-to-date list of user manual holders available for amendment and update purposes.

5.3 The Chart of Accounts provides a comprehensive, up to date listing of financial codes set up on the General Ledger system, consisting of Cost Centre and Account Codes, with all changes being subject to appropriate review and authorisation.

5.4 Data is input to the general ledger from subsidiary feeder systems, either directly or via the Payables system, in accordance with individual system timetables. All system import files accepted by the General Ledger are listed in the daily system validation and error control reports. Direct feeder systems are reviewed and monitored by the System Administrator and include Debtors, Payroll, Internal Recharges, Cash Receipting, Road Costing and Tranman .Indirect system feeds, including Payables, are all validated by other officers.

5.5 Amendments to data held on the General Ledger system are achieved by the input of journals, which can be created by staff with ‘main user’ system access rights but can only be posted by ‘Accountant’ users. The system will not accept for posting any journals with invalid codes or which do not balance

5.6 The accuracy and completeness of outputs is ensured by the production of daily Interface Log reports which confirm that input files have been successful, with any errors identified and reported for investigation and resolution by appropriate officers.

5.7 Data is protected against loss or system failure by the Council's approved mainframe security procedures with no additional back-up by the system administrator considered necessary.

6 RECOMMENDATIONS

One recommendation of Medium priority and three of Low priority were identified as a result of the audit. The recommendations are shown in the action plan attached at Appendix 2 which has been compiled with the co-operation and agreement of the Finance Manager, Corporate Support.

Internal Audit considers that, in an effort to improve the quality of information, monitoring and control, the recommendations should be implemented in accordance with the agreed action plan. Management have set achievable implementation dates and will be required to provide reasons to the Audit Committee for failure to implement within the agreed timescale. Where management decides not to implement recommendations it must evaluate and accept the risks associated with that decision.

A system of grading audit findings, which have resulted in an action, has been adopted in order that the significance of the findings can be ascertained. Each finding is classified as high, medium or low. The definition of each classification is set out below:-

High - major observations on high level controls and other important internal controls. Significant matters relating to factors critical to the success of the objectives of the system. The weakness may therefore give rise to loss or error;

Medium - observations on less important internal controls, improvements to the efficiency and effectiveness of controls which will assist in meeting the objectives of the system and items which could be significant in the future. The weakness is not necessarily great, but the risk of error would be significantly reduced it if were rectified;

Low - minor recommendations to improve the efficiency and effectiveness of controls, one-off items subsequently corrected. The weakness does not appear to affect the ability of the system to meet its objectives in any significant way.

7 AUDIT OPINION

Based on our findings we can conclude that there are appropriate controls and procedures in place to ensure the integrity and security of information input to the General Ledger although the level of control would be further enhanced by the implementation of the recommendations set out in the agreed management action plan attached at Appendix 2.

8 ACKNOWLEDGEMENTS

Thanks are due to the Strategic Finance Staff and the System Administrator for their co-operation and assistance during the course of audit and the preparation of the report and action plan.

Argyll & Bute Council's Internal Audit section has prepared this report. Our work was limited to the objectives in section 2. We cannot be held responsible or liable if information material to our task was withheld or concealed from us, or misrepresented to us.

APPENDIX 2 ACTION PLAN

No.	FINDINGS	PRIORITY	RECOMMENDATION	RESPONSIBLE OFFICER	IMPLEMENTATION DATE
4	The duties and responsibilities of the General Ledger System Administrator are not clearly documented	Medium	The role of GL System Administrator should be clarified and documented	Finance Manager, Corporate Support	30/9/2013