SCOTTISH POLICE AUTHORITY

Meeting	**Scottish Police Authority Audit Committee**
Date	**18 April 2018**
Location	**Scottish Police Authority Headquarters, Pacific Quay, Glasgow**
Title of Paper	**Financial Ledger**
Item Number	**5.3**
Presented By	**Helen Berry**
Recommendation to Members	**For Noting**
Appendices Attached	**Yes Appendix A**

PURPOSE

The purpose of this paper is to provide the Audit Committee with outcomes and proposed actions following on from the review of the financial ledger.

Scottish Police Authority

Internal Audit Report 2017/18

Financial Ledger

February 2018

Scott-Moncrieff
business advisers and accountants

Scottish Police Authority

Internal Audit Report 2017/18

Financial Ledger

Audit Sponsor	*Key Contacts*	*Audit team*
James Gray, Interim Chief Financial Officer, PS and SPA	*Sarah Jane Hannah, Head of Financial Accountancy* *Tim Pearson, Principal Development Accountant* *Graeme Barrie, Systems Administrator* *Catherine O'Connor, Accountant* *Mhairi Blair, Finance Officer*	*Gary Devlin, Partner* *Helen Berry, Head of Internal Audit* *Laura Livingston, Internal Audit Senior Manager* *Claire Beattie, Assistant Manager* *Nadia Napier, Internal Auditor* *Morag Adamson, Internal Auditor*

Executive Summary

Conclusion

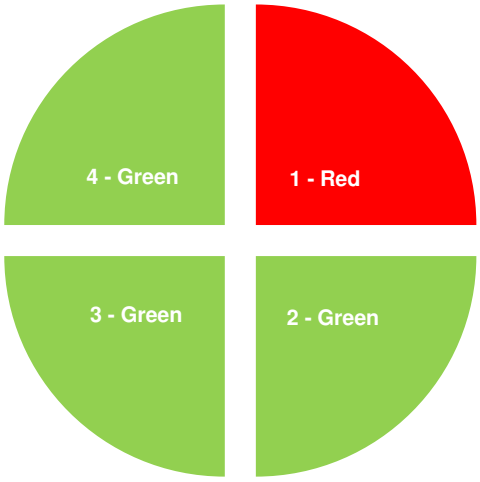
The controls over the Police Scotland financial ledger are well designed and operating appropriately for three out of four of the control objectives reviewed. However, we have identified significant control weaknesses relating to segregation of duties in relation to posting journal entries, as well as a lack of up-to-date and comprehensive policies and procedures. These two recommendations had previously been raised in our 2015/16 General Ledger – Core Financial Controls Report and have not yet been addressed by management. Three new improvement actions have also been identified through this review.

Background and scope

As a public sector organisation the Scottish Police Authority (SPA) is accountable for the proper use of the public funds. In order to ensure the economic, efficient and effective use of these monies, it is essential that SPA / Police Scotland (PS) have robust processes and procedures in place over the financial ledger.

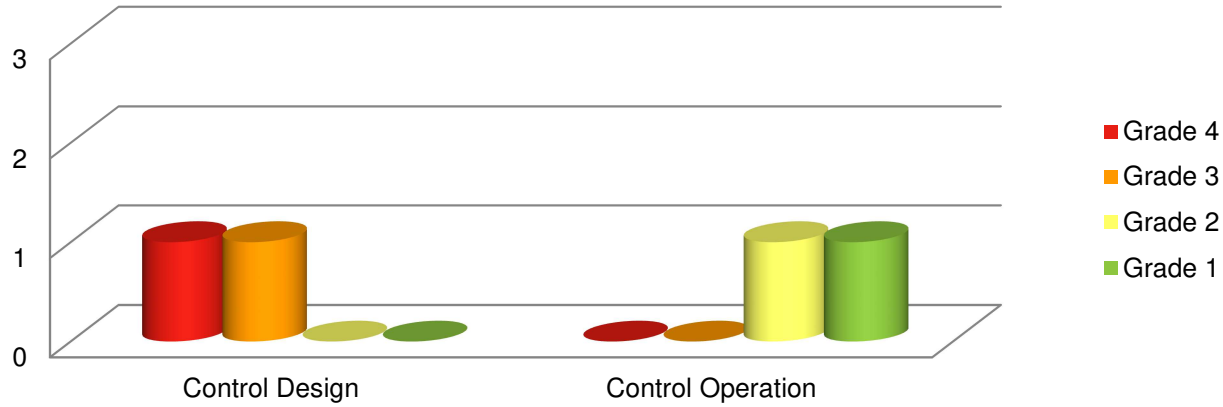
We have reviewed the controls over the financial ledger to ensure the accuracy and security over the figures reported. This included assessing the reconciliation from the feeder systems and reviewing the financial regulations in place to promote completeness and accuracy of data within the system.

Control assessment



- 1. Financial ledger accounting data is accurate, authorised, complete and up to date.
- 2. The financial ledger interfaces with other key management information systems to provide timely and accurate financial data.
- 3. The accounting data can be analysed and reported in a way that supports management decisions and actions.
- 4. Accounting records are adequately protected from loss, misuse or unauthorised amendment.

Improvement actions by type and priority



Four improvement actions have been identified from this review. Two of these actions (rated red and amber respectively) were previously identified within the 2015-16 General Ledger Core Financial Controls Report and have not been implemented by management. The two new improvement actions relate to compliance with existing procedures, rather than the design of controls themselves. Both findings outstanding from the 2015-16 review relate to control design. See Appendix A for definitions of colour coding.

Key findings

Good practice

Police Scotland's financial ledger controls procedures reflect good practice in a number of areas:

- There are automated processes in place for the payroll source data within each of the nine legacy areas to interface with the ledger. Each legacy area is required to input the payroll source data into the ledger, which has been customised to have a bespoke validation and mapping process for each legacy area. The automated process results in a journal entry being created, which is then posted by the respective legacy area.

- Management accounts are created on a monthly basis using information pulled directly from the financial ledger using the Business Objectives (Boxi) reporting tool. Management reports are run at a divisional, Assistant Chief Constable (ACC), and Deputy Chief Constable (DCC) level. As management accounts can be produced for each of these different levels, they are consistent with the organisation's operations and key business areas.

- The eFinancials user access controls are effectively designed and operated by the Systems Administrator. All new users added to the eFinancials system are required to sign a declaration contained within the Systems Operating Procedures, which is also signed by the new user's line manager. Additionally, a 'User Access Document' must be completed and signed by the new user and their line manager before the Systems Administrator processes the request.

- The Systems Administrator runs a weekly report from the system showing any users who have not changed their passwords within 12 weeks, and manually locks their user access. There is also a weekly review of the HR system (Scope) to identify any staff moving position within the organisation and no longer requiring access to eFinancials.

- There are two suspense accounts (payroll and procurement cards). The payroll suspense account is monitored, investigated and cleared on a monthly basis by the Financial Accounting Finance Officer. The procurement card suspense account is cleared on a monthly basis by the Cash and Banking team once details of BarclayCard expenditure for the month have been obtained.

- The accruals and prepayments journals posted into the ledger are reviewed by an Accountant within the Financial Accounting team on a quarterly basis. All accruals and prepayments are investigated, checked for accuracy, and an explanation for each entry into the ledger is documented. This in-depth review being completed ensures that the accrual and prepayment financial ledger accounting data is accurate and up-to-date throughout the year.

Areas for improvement

We have identified a number of areas for improvement which, if addressed, would strengthen SPA / PS's control framework. Three new improvement actions have been identified from this review. In addition, two issues which were originally identified within our 2015-16 General Ledger – Core Financial Controls Report have been highlighted as still outstanding. Findings raised include:

- Ensuring that there are segregation of duties controls implemented for inputting and posting journal entries onto the financial ledger (eFinancials);

- Reviewing, updating and including version controls within all documented policies and procedures for financial ledger processes;
- Ensuring that payroll balance sheet control account reconciliations are reviewed by a second member of staff;

These are further discussed in the Management Action Plan below.

Acknowledgements

We would like to thank all staff consulted during this review for their assistance and co-operation.

Management Action Plan

Control Objective 1: Financial ledger accounting data is accurate, authorised, complete and up to date.

Red

1.1 Journal Entry Segregation of Duties (SoD)

The controls in place for segregation of duties between staff inputting and posting journals onto the financial ledger system (eFinancials) are not operating effectively. The eFinancials system automatically documents the staff member who inputs the journal into the system (the 'originator'), and the member of staff who authorises or posts the journal (the 'authoriser'). We understand that there is functionality within the eFinancials system to enforce segregation of duties by requiring the originator and authoriser to be separate individuals however this functionality has not been enabled as evidenced throughout our detailed testing.

There is a standard journal entry form available on the staff intranet, which should be completed for journal entries. This template should be completed fully before a journal entry is posted to the ledger and contains cells for the staff members who prepared and authorised the journal to enter their details. This procedure is designed to ensure that there is appropriate oversight by the authoriser that the proposed journal is correct however our detailed testing confirmed that this control is not operating effectively.

In addition, adequate supporting documentation should be retained for each journal, to provide a sufficient audit trail as outlined in the Budget Management and Month End Guidelines.

However, our testing of a sample of 24 journal entries posted to the system in 2017/18 found several instances in which these controls were not operating effectively:

- One of the journal entries tested was an automated (POP Accrual) journal, which did not require segregated authorisation. Of the remaining 23 journals the originator and authoriser was the same individual in four instances and only the originator was recorded in the remaining 19.
- We found a lack of consistency in relation to completion of the journal template forms, which should be completed before the journal is posted to the ledger. The automated journal (POP accrual) does not require a completed journal entry form. Three of four payroll journal entries did not have a documented journal entry form, while the fourth had a form that was not counter-signed as completed or authorised. Seventeen journal entry forms were either left blank or only signed by one person. Only two journal entry forms were documented and checked by separate members of staff.
- Insufficient backup was provided for 6 of the 24 journal entries tested, which is not in line with the documented Budget Management and Month End Guidelines.
- Our review of the backup evidence provided identified one incorrect journal. Backup documentation showed that a line of £850 was excluded from the journal posted into the financial ledger. This journal template had been completed by one member of staff. This same member of staff then posted the journal entry into the financial ledger, with no secondary authorisation of the journal by a second member of staff.

Since the end of June 2017, listings of the journal entries posted for the month are run from the financial ledger (Boxi report) by a Financial Accounting Accountant. This listing is then emailed to the Finance Managers to

allow them to review the journals posted during the period. However there is no requirement for the Finance Managers to confirm that they have completed the monthly review and are satisfied that the journals are accurate or, conversely, have identified discrepancies for further investigation. We do not consider this to be an effective control.

In addition to our sample testing, we obtained a listing of all journals posted in 2017/18 (up to period 10) and analysed the data for correcting journals. A total of 10,306 journals, with a value of £3.7 billion were posted to the general ledger in this period. Of these, 586 journals (5.7%), with a value of £45.7million were found to contain our key search words.

Risk

Inadequate segregation of duties increases the risk that unauthorised, erroneous or fraudulent journals are posted to the financial ledger. It also reduces the efficiency of the finance processes due to the increased requirement for correcting journals.

Recommendation

This issue was previously raised within our 2015/16 General Ledger – Core Financial Controls Report (2.1 Segregation of Duties (SoD)/Authorisation), where we recommended that segregation of duties should be enforced over each key financial control process (including journals) to ensure fraudulent transactions and errors cannot be created and posted to the ledger without being detected.

As a result, we have not raised an additional recommendation within this report. However, we again highlight the lack of controls within this area and strongly recommend that management prioritise this action.

We recommend that management consider investigating the functionality within eFinancials to enforce segregation of duties by setting up the requirement that the originator and authoriser are separate individuals. This would negate the need to have both a preparer and authoriser sign off on the standard journal entry form which would lead to increased efficiencies.

Management Action

Grade 4 (Design)

Action owner: Financial Transactions Lead **Due date:** July 2018

Management accept this recommendation. There is a compensating control in place through the month end review of all manual journals undertaken by management, however we recognise that this control is not currently operating effectively. We will review this control and ensure that the checks are formally signed off to evidence completion, including the investigation of any unusual journals identified. Furthermore we will investigate the possibility of introducing functionality on eFinancials to implement an automated process for the authorisation of individual journals.

Action owner: Statutory Reporting Lead **Due date:** July 2018

The Financial Accounting Team will introduce an additional sign-off of monthly journals by the Tier 3 managers incorporating spot-checks to ensure there is adequate backup, providing an additional level of review conducted each month.

1.2 Policies and Procedures

We reviewed the financial ledger procedures available on the staff intranet, including Security Operating Procedures, Budget Management and Month End Guidelines, Xcel Uploader Guidance, eFinancials Reference Guide and eFinancials GL Training Notes. We noted:

- Three of the procedure documents reviewed (Security Operating Procedures, Budget Management & Month End Guidelines and eFinancials Reference Guide) have documented version controls. The Budget Management & Month End Guidelines were updated in July 2017, the Security Operating Procedures were updated in September 2016 and the eFinancials Reference Guide was updated in 2013.
- The General Ledger training notes overlap with other documented guidance on the intranet – the Xcel Uploader Guidance. Neither of these documents have version controls which state the date of last review.
- During the review, the Financial Accounting Finance Officer provided us with procedure notes for payroll reconciliations however these are still in draft form and have not been completed or approved.

Our review of the documentation in place did not identify any procedures for the authorisation of journals. Furthermore, our discussions with members of the staff within the Finance Team highlighted that there was a lack of awareness of the policies and procedures available on the intranet.

Risk

Outdated policies and procedures and a lack of documented procedures can lead to confusion for employees looking to reference a particular procedure. There is a risk that inconsistent procedures are followed and a lack of uniformity exists across the organisation which could lead to unauthorised and erroneous journals being posted to the financial ledger.

Recommendation

This issue was previously raised within our 2015/16 General Ledger – Core Financial Controls Report (1.1 Policies and Procedures), where we recommended that management should ensure policies and procedures are in place for all financial processes. Policies and procedures should be reviewed and updated on at least an annual basis. Each policy and procedure should have a revision log stating the date of the last review and next review.

As a result, we have not raised an additional recommendation within this report. However, we again highlight the weakness in controls within this area and strongly recommend that management prioritise this action.

Management Action

Grade 3 (Design)

Action owner: Statutory Reporting Lead **Due date:** July 2018

Management accept this recommendation. The eFinancials system has been awaiting an upgrade to eFinancials which has been subject to serious delay. The Systems Development Team will be reviewing all finance policies and procedures during the first quarter of 2018/19 to ensure they are appropriate, up to date, and reflect best practice.

1.3 Second review of Payroll Control Account Reconciliations

The payroll information in the general ledger is reconciled to the nine legacy payroll systems on a monthly basis. Strathclyde and SPA payroll is processed at the Police Scotland office at Dalmarnock, and the Financial Accounting Finance Officer completes the reconciliations for these two legacy areas. All other legacy areas need to upload the payroll source data into eFinancials. Grampian, Tayside and Forth Valley complete the payroll control account locally, while Dumfries & Galloway, Fife, Edinburgh & Lothian, and Inverness payroll control accounts are completed by the Financial Accounting Finance Officer in Dalmarnock.

Our testing of a sample of nine 2017/18 payroll control account balance sheet reconciliations, across each of the nine payroll legacy areas found that there was no secondary review of the Payroll Control Account reconciliations being performed.

Risk

There is a risk that errors in the completion of payroll control account reconciliations are not picked up due to a lack of secondary review. Furthermore, a lack of secondary review increases the risk that reconciling items are not addressed appropriately and on a timely basis.

Recommendation

All payroll control account reconciliations should be performed and reviewed by two separate members of staff, ensuring adequate segregation of duties. Completion and review of the payroll control account reconciliations should take place in a timely manner.

Management Action

Grade 2 (Operation)

Action owner: Statutory Reporting Lead **Due date:** July 2018

Management accept this recommendation. The Financial Accounting Team will introduce an additional second level review of the monthly payroll balance sheet control account reconciliations after completion of the year-end work in June 2018.

Control Objective 2: The financial ledger interfaces with other key management information systems to provide timely and accurate financial data

No weaknesses identified

Payroll systems are maintained by each of the 9 legacy areas as outlined above. There are automated processes in place for the payroll source data to interface with the ledger. Each legacy area is required to input the payroll source data into the ledger, which has been customised to have a bespoke validation and mapping process for each legacy area. The automated process results in a journal entry being created, which is then posted by the respective legacy area.

Testing performed during the audit included confirming payroll source data to the financial ledger for a sample of payroll runs across all legacy areas. For all sample items tested, the payroll source data was accurately included within the financial ledger. We performed detailed testing over payroll values across all of the nine legacy areas. Sample items were chosen across each of the different payroll streams (e.g. support staff/officers/executives), and across the 2017/18 financial period up until period 10.

The sales ledger and purchase ledger systems used are eFinancials. Therefore, any data inputted into the sales or purchase ledger automatically updates information into the general ledger. This process is automated which minimises the risk of variances occurring between the systems. Testing confirmed that the Finance team checks that the sales and purchase ledgers are accurately interfacing with the general ledger on a monthly basis.

As part of the month end close down procedures, the sub-ledgers (including the sales ledger and purchase ledger) have to reconcile with the general ledger in order to be rolled forward to the next period. Therefore, this control would identify whether the sub-ledgers are not accurately interfacing with the ledger.

Control Objective 3: The accounting data can be analysed and reported in a way that supports management decisions and actions

Green

No weaknesses identified

Management accounts are created on a monthly basis using information pulled directly from the financial ledger using the Business Objectives (Boxi) reporting tool. Management reports are run directly from the eFinancials system at a divisional, Assistant Chief Constable (ACC), and Deputy Chief Constable (DCC) level, providing consistency with the organisation's operations and key business areas.

Senior management (e.g. Assistant Chief Constables) can produce reports directly from the system which includes all of the lower level divisional data, reducing the risk of data manipulation before review by higher levels within the organisation. The hierarchy system is built into the Boxi system, with only the cost centre and the period having to be manually input to identify which report should be run. Reports can be run at any time allowing relevant, appropriate and timely information to be produced for management.

The only part of the management accounts not directly produced from Boxi (eFinancials) are the forecasts and narrative explanations for any variances identified. Forecasts are input by each division/region based on specific divisional knowledge.

A review of a sample of divisional, ACC and DCC management accounting reports produced confirmed that the management accounts include key financial information such as annual budget, YTD budget, YTD expenditure, year-end forecasts, prior year actual figures, current month expenditure, current month budget as well as other useful information such as overtime figures.

Control Objective 4: Accounting records are accurately protected from loss, misuse or unauthorised amendment.

Green

4.1 System Administrator Cover for Weekly Controls

There are strong weekly controls in place to identify the staff members that should have their access rights to the financial ledger removed. The Systems Administrator has a controls checklist in place which includes:

- Obtaining a report from the system identifying all users who have not changed their passwords within the past 12 weeks; and
- Obtaining a report from the HR system (Scope) identifying all users who have changed roles and therefore no longer require access to eFinancials.

Sample testing identified that the weekly controls outlined above were not performed in a timely manner during the period of July 2017; this coincided with the Systems Administrator being on a period of leave. We confirmed that the financial ledger user access controls were completed when the Systems Administrator returned to work at the beginning of August. Management asserted that there are two other members of the Finance Team who have Systems Administrator access to eFinancials who would be able to cover for the Systems Administrator during leave periods however this did not occur in July 2017 due to a lack of training.

Risk

Management Action

Grade 1 (Operation)

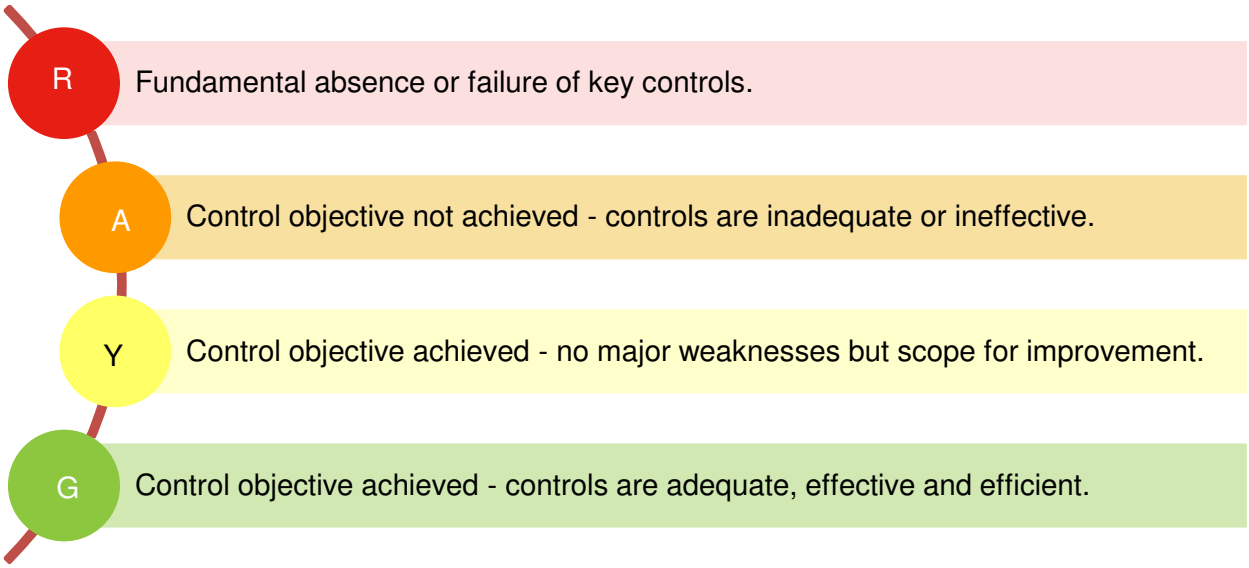
Action owner: Statutory Reporting Lead **Due date:** March 2019 (Interim measure implemented – March 2018)

Management accept this recommendation. The finance team are currently being restructured, with systems administration being under review as part of that restructure. Permanent cover for all systems administration will be stabilised at that time.

In order to alleviate this is the shorter term; training has been carried out with a member of the Financial Accounting Team to ensure adequate cover for the one systems administrator.

Appendix A – Definitions

Control assessments



Management action grades

4	•Very high risk exposure - major concerns requiring immediate senior attention that create fundamental risks within the organisation.
3	•High risk exposure - absence / failure of key controls that create significant risks within the organisation.
2	•Moderate risk exposure - controls are not working effectively and efficiently and may create moderate risks within the organisation.
1	•Limited risk exposure - controls are working effectively, but could be strengthened to prevent the creation of minor risks or address general house-keeping issues.