



Creditors

Peak District National Park Authority

Internal Audit Report 2016/17

Business Unit: Finance
Responsible Officer: Director of Corporate Strategy & Development
Service Manager: Head of Finance
Date Issued: 23 March 2017
Status: Final
Reference: 69130/002

	P1	P2	P3
Actions	0	0	2
Overall Audit Opinion	Substantial Assurance		

Summary and Overall Conclusions

Introduction

Creditor payments is a key service within the council. Creditor payment systems form a regular part of the audit plan as a main financial system, due to the potential for fraud.

As well as reviewing creditors procedures the audit examined the authority's compliance with procurement rules.

Objectives and Scope of the Audit

The purpose of this audit is to provide assurance to management that procedures and controls within the system will ensure that:

- Invoices are properly raised, certified and authorised
- Invoices are paid in a timely manner
- Procurement rules have been followed in regards to paying invoices
- There are sufficient controls in place to prevent supplier bank account details

Key Findings

A sample of 20 payments identified that each one is supported by a purchase order which matched the purchase detail on the invoice. Each of the invoices was authorised by an individual or committee before the payment had been completed. The authority record data on the time difference between the date invoices have been received and the date the invoices have been paid. Under the late payment act invoices have to be paid within 30 days. In 2008/09 the Authority paid 94.27% of invoices within 30 days since then the number of invoices paid within 30 days has decreased each year, in 2015/16 the amount of invoices paid within 30 days was 92%.

Within our sample we found that the procurement rules had been followed correctly with the exception of one payment that was part of a contract, that was initially for a 3 year period commencing in 2007. The contract has currently rolled over for 7 years following the expiry of the initial contract period.

The authority have a process in place to verify that change of bank detail notification letters sent to the authority are verified before bank details are changed on the financial system. However there are two instances where there was no evidence that the process had been followed correctly.

Overall Conclusions

The arrangements for managing risk were good with few weaknesses identified. An effective control environment is in operation, but there is scope for further improvement in the areas identified. Our overall opinion of the controls within the system at the time of the audit was that they provided Substantial Assurance.

1 Changing bank account details.

Issue/Control Weakness

The Authority has not followed the procedure for changing supplier bank details. In addition to this insufficient information is being recorded when the Authority changes supplier bank details.

Risk

Supplier bank details are changed to the bank details to a fraudulent bank account. This would lead to loss of money for the authority.

Findings

When a letter/e-mail is received from a supplier stating that their bank account has changed the authority verifies that the letter/e-mail is genuine by phoning the supplier to check they have changed their bank details, before updating the supplier details on the finance system. We found two occasions from our sample of 10 where the authority have not recorded that they have verified if suppliers change of bank account details were genuine.

It is important to ensure that the details are checked using contact details obtained independently from the request before making the change. Currently records do not provide details of how contact details were sourced, and the name of the person who verified the change. At the time of the audit it was accepted that better guidance was required on verifying details and recording evidence, although there is no formal timescale to produce new guidance.

Agreed Action 1.1

Agreed

Priority

3

Responsible Officer

Finance Officer

Timescale

31st July 2017

2 Expired contract

Issue/Control Weakness

A contract has been extended for numerous years.

Risk

The supplier cannot be held accountable for the work they are carrying out. This would mean that the authority is not getting the best value for money.

Findings

A sample of 20 payments was reviewed to ensure procurement rules had been followed based upon the value of the payment. One payment for £10,280.25 relates to a maintenance contract for 19 Car Park Pay and Display Machines with the supplier Parkeon Limited. The contract was for a 3 year period from August 2007, with the potential to roll on the contract, but the invoice covers the period 4/8/14 to 3/8/16.

Agreed Action 2.1

The Contract will be renewed.

Priority

3

Responsible Officer

Head of Visitor
Experience

Timescale

31st March 2018

Audit Opinions and Priorities for Actions

Audit Opinions

Audit work is based on sampling transactions to test the operation of systems. It cannot guarantee the elimination of fraud or error. Our opinion is based on the risks we identify at the time of the audit.

Our overall audit opinion is based on 5 grades of opinion, as set out below.

Opinion	Assessment of internal control
High Assurance	Overall, very good management of risk. An effective control environment appears to be in operation.
Substantial Assurance	Overall, good management of risk with few weaknesses identified. An effective control environment is in operation but there is scope for further improvement in the areas identified.
Reasonable Assurance	Overall, satisfactory management of risk with a number of weaknesses identified. An acceptable control environment is in operation but there are a number of improvements that could be made.
Limited Assurance	Overall, poor management of risk with significant control weaknesses in key areas and major improvements required before an effective control environment will be in operation.
No Assurance	Overall, there is a fundamental failure in control and risks are not being effectively managed. A number of key areas require substantial improvement to protect the system from error and abuse.

Priorities for Actions

Priority 1	A fundamental system weakness, which presents unacceptable risk to the system objectives and requires urgent attention by management.
Priority 2	A significant system weakness, whose impact or frequency presents risks to the system objectives, which needs to be addressed by management.
Priority 3	The system objectives are not exposed to significant risk, but the issue merits attention by management.

Where information resulting from audit work is made public or is provided to a third party by the client or by Veritau then this must be done on the understanding that any third party will rely on the information at its own risk. Veritau will not owe a duty of care or assume any responsibility towards anyone other than the client in relation to the information supplied. Equally, no third party may assert any rights or bring any claims against Veritau in connection with the information. Where information is provided to a named third party, the third party will keep the information confidential.