Fraud Risk Assessment

Final Report

Auditor	Alice Gibson Andrew Collins
Contact Details	Tel: 01924 294061 Alice.Gibson@westyorkshire.pcc.pnn.gov.uk Andrew.Collins@westyorkshire.pcc.pnn.gov.uk
Date of Review	December 2014 to February 2015
Draft Report Issued	5 March 2015
Final Report Issued	23 June 2015

1. Executive Summary

The Organisation has acted pro-actively and sanctioned Internal Audit to conduct an exercise to identify and assess the Organisations fraud risks. This report presents the fraud risk assessment, highlighting the potential fraud risks that the Organisation may be exposed to and sets out the proposed future use of the assessment as part of an overall anti-fraud and corruption strategy that is considered best practice by bodies such as the Chartered Institute of Public Finance & Accountancy (CIPFA), the Institute of Internal Auditors (IIA) and the Chartered Institute of Management Accountants (CIMA) amongst others.

The implementation of a strategic approach to understanding and managing the risk of fraud facilitates the improvement of the control environment, helps drive out potential waste and abuse and assists in achieving the objective of minimising the risk to the Organisation of the occurrence of fraud.

- For information on the context of organisational fraud see *Appendix 2.*
- For an explanation of the key steps to implementing an effective fraud strategy see *Appendix 3.*

Fraud Risk Assessment - Methodology

The initial stage of the Fraud Risk Assessment was to identify the fraud risks to the Organisation. This was achieved through evaluating business areas for fraud risk, reviewing findings from existing audit reports, consulting Organisation staff, using information on historic cases of fraud known to the Professional Standards Department and a knowledge of generic fraud risks in public & private sector organisations.

The assessment involved examining multiple business systems and processes throughout the Organisation for risks of potential fraud and scoring the risk according to the Organisation's risk appetite criteria. The criteria included likelihood of occurrence and the legal, financial, reputational and operational implications. The fraud risks have been scored both inherently and residually.

To utilise the Fraud Risk Assessment it is important to be aware of the differences between Inherent and Residual Risk.

Inherent Risk

In respect of fraud, this is the risk that a fraud scheme would pose if **no controls** or other mitigating factors were in place. Essentially risk before controls.

Residual Risk

This is the risk that remains **after controls** are taken into account.

The fraud risks, have been scored in line with the Organisation Risk Scoring Matrix (*Appendix 1*), allowing them to be categorised as High, Medium or Low Risk. The results have been plotted graphically for ease of presentation and tabulated to highlight the level of improvement resulting from the presence of the actual mitigating controls.

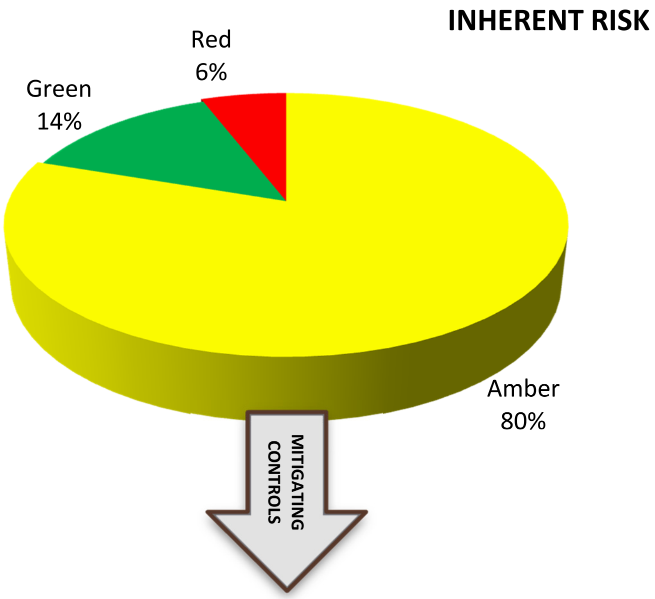
1.1 Impact of Mitigating Controls on Fraud Risk Level

The fraud risk assessment established that on the whole controls in place throughout the Organisation are robust, appropriate and fit for purpose in managing the inherent risk of fraud and corruption to a more acceptable residual level.

Figure 1 shows that the Organisations exposure to **inherent** risk is 6% High risk, 80% Medium risk, and just 14% Low risk. However, once mitigating controls and factors are taken into account the Organisation **residual** risk exposure is much lower with just 17% Medium risk and 83% Low risk. This indicates that controls in place are having a positive effect on the Organisations risk exposure.

It is not possible to determine whether the controls are as effective as the Organisation would wish without the Organisation making a determination as to their acceptable risk level for each scheme. It is recommended that the Organisation undertake an exercise to determine their acceptable risk level for each scheme, this would then allow excessive control to be reduced, resulting in more efficient use of resource and where the desired risk level is not being achieved allow the Organisation to target resource at these areas. The fraud risk assessment provided allows the Organisation to perform this exercise and also provides a gap analysis so that areas for improvement can be readily identified.

Figure 1 – Risk Improvement through mitigating controls



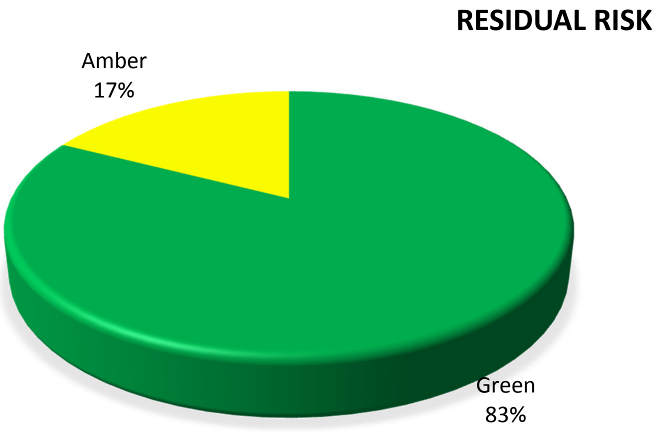

RESIDUAL RISK
Amber
17%
Green
83%

Table 1 details the individual fraud risk schemes by area, their assessed risk category alongside their inherent and residual risk scores. Mitigating controls and factors for all fraud risk schemes identified resulted in a lowered risk score, as can be seen in the Inherent and Residual Risk scores columns, the difference between inherent and residual risk scores provides a rough indicator as to how much the risk reduced as a consequence of mitigating controls and factors.

The vast majority of fraud risk schemes saw a reduction in their respective risk category e.g. High, Medium and Low Risk, these results indicate that controls that the Organisation has in place are effective in reducing Organisation exposure to fraud risk.

A future assessment has been performed to assess the category that risk schemes are anticipated to sit once any outstanding management actions are successfully implemented. The assessment indicates that where a drop is possible that the majority of risk schemes see a reduction in their respective category.

Table 1 – Risk improvement through mitigating controls

	Inherent Score	Residual Score	Future Score
Billing schemes			
Using fictitious suppliers or shell companies for false billing.	9	6	🟩
Pay and return schemes (where an employee creates an overpayment to a supplier and pockets the subsequent refund).	4	2	🟩
Bribery			
Change order abuse	9	6	🟩
Giving and accepting payments to favour or not favour other commercial transactions or relationships.	9	6	🟩
Authorising orders to a particular supplier in return for bribes.	9	6	🟩
Cheque fraud			
Theft of cheques.	9	1	🟩
Tampering with cheques (payee/amount).	9	1	🟩
Depositing a cheque into a third party account without authority.	4	1	🟩
Duplicating or counterfeiting of cheques.	6	1	🟩
Crime - Inventory and fixed assets			
Theft of property upon disposal	9	9	🟩
Theft of Money upon disposal	9	9	🟩
Theft of drugs upon disposal	9	9	🟩
Theft of Firearms upon disposal	9	9	🟩
Extortion			
Extortion (offering to keep someone from harm in exchange for money or other consideration).	9	8	🟧
Blackmail (offering to keep information confidential in return for money or other consideration).	12	8	🟧
False Claims			
False public Compensation claims	9	6	🟩
False payment requests			
False email payment request together with hard copy printout with forged approval signature.	9	6	🟩
Employee creating false payment instruction with forged signatures and submitting it for processing.	9	6	🟩
Inventory and fixed assets			
Theft of Firearms from evidence stores	9	9	🟩
Theft of Drugs from evidence stores	9	9	🟩
Theft of Cash from evidence stores	9	9	🟩
Theft of Property from evidence stores	9	9	🟩
Unauthorised private use of Organisation property.	9	6	🟩
Receiving free or below market value goods and services from suppliers.	9	6	🟩
Theft of fixed assets, including computers and other IT related assets.	9	6	🟩
False write offs/disposals and other debits to inventory.	9	6	🟩

	Inherent Score	Residual Score	Future Score
Theft of inventory.	9	6	
Inability to explain and/or itemise expenditure on assets	9	3	
Kickbacks			
Purchase of property at higher than market value in exchange for a kickback.	9	6	
Unnecessary purchases	9	6	
Unjustified single source	9	6	
Kickbacks to employees by a supplier in return for the supplier receiving favourable treatment.	9	6	
Employee sells Organisation-owned property at less than market value to receive a kickback or to sell the property back to the Organisation at a higher price in the future.	9	6	
Preferential treatment of customers in return for a kickback.	9	6	
Misuse of accounts			
Stealing passwords to payment systems and inputting series of payments to own account.	9	6	
Wire transfer fraud (fraudulent transfers into bank accounts).	9	6	
Unrecorded sales or receivables.	6	4	
Writing false credit note to customers with details of an employee’s personal bank account or of an account of a company controlled by the employee.	4	1	
Non-financial			
Falsified employment credentials e.g. qualifications and references.	9	3	
Other accounting misstatements			
Non clearance or improper clearance of suspense accounts.	9	3	
Misrepresentation of suspense accounts for fraudulent activity.	9	3	
Payroll			
Payment of deceased pensions	9	6	
Forging/false sick notes	9	6	
Submitting inflated or false expense claims.	9	6	
Adding private expenses to legitimate expense claims.	9	6	
Improper changes in salary levels.	9	6	
Applying for multiple reimbursements of the same expenses.	9	6	
Retention of salary overpayment	9	6	
Employment under false pretences	9	6	
Working on sick leave	9	6	
False workers’ compensation claims.	9	6	
Fictitious (or ghost) employees on the payroll.	9	6	
Abuse of holiday leave or time off entitlements.	6	4	
False pension accounts	9	3	
Roster manipulation for allowances	9	3	
Falsifying work hours to achieve fraudulent overtime payments.	9	3	
Theft of employee contributions to benefit plans.	6	2	
Personal interests			
Collusion with customers and/or suppliers.	9	6	
Favouring a supplier in which the employee has a financial interest.	9	6	
Employee hiring someone close to them over another more qualified applicant.	9	6	
Procurement			
Unauthorised Purchasing	9	9	
Defective Quality Goods / Services	9	6	
Falsifying documents to obtain authorisation for payment.	9	6	
False or duplicate invoices from suppliers	9	6	
Forging signatures on payment authorisations.	9	6	
Marked up invoices from contracts awarded to supplier associated with an employee.	9	6	
Improper changes to supplier payment terms or other supplier details.	9	6	
Purchases for personal use / resale.	9	6	
Cover pricing	9	6	
Submitting for payment false invoices from fictitious or actual suppliers.	9	6	
Altering legitimate purchase orders.	9	6	

	Inherent Score	Residual Score	Future Score
Invoices for goods or services not supplied	9	6	
Improper use of Organisation credit cards.	9	6	
Inappropriate use of consultant staff	9	6	
Intercepting payments to suppliers.	9	3	
Sending fictitious or duplicate invoices to suppliers.	9	3	
False creation of suppliers	9	3	
Procurement – Jointly managed between the Organisation and Regional Procurement			
Anti-trust activities such as price financial fixing or bid rigging.	12	8	
Price fixing between suppliers	12	8	
Sale of critical bid information, contract details or other sensitive information.	12	8	
Vendor market sharing	12	8	
Theft of cash			
Stealing from IMPREST	3	1	
False IMPREST claims	3	1	
Stealing from petty cash.	3	1	
Inappropriate use of IMPREST cash	6	1	
Skimming of cash before recording revenues or receivables (understating sales or receivables).	3	1	

2. Key observations identified through the Fraud Risk Assessment

The fraud risk assessment identified a number of areas where the Organisation is unreasonably exposed to the risk of fraud and corruption, and therefore corrective action should be considered:

Evidence Stores

- The evidence stores were considered as part of the review, utilising information from previous audit work the assessment identified that should drugs, money and property be misappropriated it is unlikely this activity would be detected in timely manner, if at all.
- The 2010 Sensitive Property Audit and the 2013 Niche Exhibits Audit identified weaknesses including non-adherence to drugs management procedures, poor key security, inadequate maintenance of property records and use of Excel spreadsheets as primary records.

Compensation Claims

- Gallagher Bassett Compensation Recovery Unit performed an audit on the Organisations processes around compensation claims. Their audit report stated that the Organisation has no formal counter fraud process in place and that there was little visible evidence on claim files to suggest that fraud is being considered when dealing with compensation claims. This suggests that the Organisation is not giving due consideration to the fact that compensation claims received may be fraudulent and is therefore leaving itself exposed to fraudulent claims.
- Gallagher Basset recommended that the Organisation develop an internal counter fraud process to ensure that all claims are screened for potential fraud and that this is recorded on the file.

Payroll

- Currently the creation of all new employees and employee detail amendments are actioned by payroll following a request from HR. These actions are independently checked by a colleague to the paperwork received from HR, however, were an individual to set up a ghost employee or amend employee details and not submit it for checking then there would not be anything to prompt a check.
- This issue has previously been raised in the 2014 Payroll Audit with a recommendation of generating a system listing from the payroll system of all newly created employees or employee amendments and checking these to supporting documentation.

Local Procurement

- The assessment found that where local procurement uses the I-Procurement system and associated operating processes that strong controls are in place, effectively mitigating a number of procurement fraud schemes such as false invoicing, overcharging and inappropriate purchasing etc.

- The December 2014 Financial Systems Assurance Audit identified that 43% of local procurements bypassed the I-Procurement system and processes. Many of these transactions are not required to have an order by the Organisation and on that measure, 10% that required an order bypassed the I-Procurement system and did not have an order.
- This bypass increases the Organisations exposure to fraud risk schemes such as false or duplicate invoicing, false payment authorisation, inappropriate purchasing, unauthorised purchasing and schemes involving supplier and purchaser collusion. The bypass weakens segregation of duty controls including approvals and authorisations, eliminates approved supplier controls, eliminates the system mandated 3 way match between ordering, goods receipt and invoices. The net effect is that reliance is placed on unknown local controls and control emphasis shifts more toward detection from prevention.
- Additionally the bypass results in a significantly more inefficient process.

Regional Procurement

- The Organisation carries a number of relatively high scoring risks in respect of large scale procurement fraud risk schemes; these are schemes such as Price Fixing between suppliers, Market Sharing, Cover Pricing and Inappropriate Tender Activity. Such fraud risks affect all areas of the public sector and are recognised as being extremely difficult to detect let alone control. The audit established that Regional Procurement staff have not received Fraud Awareness training. Best practice, as stipulated by the National Fraud Authority 2011 Procurement Fraud in the Public Sector advises that counter fraud training is an invaluable weapon in an organisations anti-fraud arsenal.

3. Report Distribution

Name / Role	Draft	Final	Final with Response
Joanna Carter, Chief Executive Officer	✗	✓	✓
Det. Superintendent Maria Taylor, Head of PSD	✓	✓	✓
Jane Palmer, Chief Constables Chief Finance Officer	✓	✓	✓
Michael Porter, Commissioners Chief Finance Officer	✓	✓	✓
Risk & Assurance Unit	✗	✓	✓

4. Observations

4.1 Obtaining and maintaining value from the Fraud Risk Assessment

<table>
<tr><th colspan="3">Risk Exposure</th><th colspan="3">Root causes</th></tr>
<tr><td colspan="3">Fraud risk is not sufficiently identified and mitigated. Use of resource is not optimal.</td><td colspan="3">Absence of a risk based, strategic approach to counter-fraud.</td></tr>
<tr><th>Probability</th><th>Financial</th><th>Reputation</th><th>Operational</th><th>Legal</th><th>Rating</th></tr>
<tr><td>Probable</td><td>Significant</td><td>Significant</td><td>Significant</td><td>Significant</td><td>9 (3: 13)</td></tr>
</table>

Fraud is a dynamic crime, evolving as fraudsters react to counter fraud activity. To tackle it effectively the FRA needs to be periodically updated to account for changes in fraud and control environments.

The Fraud Risk Assessment should be a key part of the overall Organisation Anti-Fraud Strategy; and require regular updating and review, ideally at least on an annual basis. The outcome of the assessment should be reported as part of future Audit Committee meetings under existing reporting arrangements.

The overall aim of the fraud risk assessment is to provide the information required for the Organisation to take a structured and targeted approach to minimising the risk of losses to fraud and strengthen the overall control environment. The fraud risk assessment should form a key part of the Organisations approach to raising fraud awareness and effectively managing fraud risk throughout the Organisation.

The fraud risk assessment should be used to: -

- Develop fraud advisory activity to support those business areas containing the highest levels of fraud risk e.g. Procurement and Payroll.
- Inform anti-fraud and fraud prevention contributions to Organisational learning.
- Develop fraud prevention and fraud awareness activity.
- Inform both the annual audit and an anti-fraud work programme, highlighting areas for risk based reviews.
- Select areas of the business in which to deploy audit resources.
- Identify systems for pro-active fraud identification e.g. Payroll and I-Procurement.
- Prioritise areas for counter fraud investigations by the Professional Standards Department and Internal Audit.
- Select Organisation projects, boards etc. for representation by control experts such as Internal Audit and the Professional Standards Department to offer advice on the control environment so that effective controls can be pro-actively implemented into systems and projects.

It is the view of Internal Audit and widely regarded as recognised best practice by organisations including CIPFA, CIMA and the Fighting Fraud Locally Government Oversight Board that a fraud risk assessment should form part of the overall risk management arrangements of an organisation.

The assessment should be used to ensure that business areas highlight their fraud risks and have put in place appropriate mitigating measures – For more context around organisational fraud see *Appendix 2.* For a more detailed explanation of the key steps to implementing an effective fraud strategy see *Appendix 3.*

Recommendation 1

The Organisation should adopt the fraud risk assessment and assign formal responsibility for its maintenance to a given individual / department.

Periodic updating of the assessment should be undertaken in order to retain relevance through taking account of both the changing fraud and control environments and the evolving structure of the Organisation.

The results of the fraud risk assessment should be used to help guide anti-fraud activity.

4.2 Evidence Stores

Risk Exposure			Root causes		
Misappropriation of evidential property from stores.			• Flawed record keeping and maintenance		
Probability	**Financial**	**Reputation**	**Operational**	**Legal**	**Rating**
Probable	Negligible	Significant	Minor	Negligible	9 (3: 13)

Misappropriation from evidence stores is a fraud risk that carries with it particularly damaging reputational implications for the police. There have been several high profile occurrences within this region over the last few years.

Utilising information from the Sensitive Property, Niche Exhibits and Property Handling-Drugs audits, the fraud risk assessment established that the evidence stores within the Organisation harbour a number of weaknesses that make them vulnerable to fraud through misappropriation.

The Niche Exhibits audit found that on the whole the current approach, where Niche is used, is effective. Niche enables complete and accurate system changes to be logged and assures a sufficient audit trail of items, as long as procedures are complied with from the creation of entries to their eventual disposal. The audit, whilst acknowledging the strong controls in place did make a number of recommendations in order to further enhance the controls, promulgate best practice and remedy a small number of low level control breaches.

The Property Handling – Drugs audit found that Organisation drugs management procedures were not always followed. Internal Audit considered that property handling in relation to drugs management was not effective in all areas and as a result, were only able to provide limited assurances. The opinion was primarily based upon an inability to readily locate items. This was found to be due to property records not being accurately maintained.

The Property Handling – Drugs audit identified that a large backlog of drugs evidence had been allowed to accumulate, with an estimated disposal processing time of one year. The prolonged retention of drugs increases Organisation exposure to misappropriation of desirable items that inherently carry a significant reputational impact should they be misappropriated.

The audits across the evidence stores identified that records are not always accurately maintained to account for the movement of items, this increases the potential for items to be misappropriated as records cannot be completely relied upon.

The Niche Exhibits audit identified that Organisational Support Officers were updating Niche to state officers had taken items, however, verification from the officer in question was not always completed. Consequently items could be misappropriated and assigned to an officer without their knowledge.

The Organisation uses spreadsheets to record drug evidence, this represents a vulnerability as entries can be amended and/or deleted. Additionally the spreadsheet itself can also be deleted and do not retain an audit trail of access and amendments.

The audits identified that Drugs Liaison Officers could sign to state an officer has taken an item and then misappropriate it along with the evidence bag that the officer would usually sign to indicate they have taken something. There would be nothing to support the officer and should the issue be identified it would come down to one person's word against another's.

RECOMMENDATIONS MADE PREVIOUSLY IN OTHER AUDITS

4.3 Procurement

Risk Exposure			Root causes		
Misappropriation of assets			• Complexity and diversity of Procurement Fraud Schemes • Lack of appropriately fraud trained procurement personnel. • Orders not raised on I-Procurement system		
Probability	**Financial**	**Reputation**	**Operational**	**Legal**	**Rating**
Probable	Significant	Minor	Minor	Negligible	9 (3: 13)

Procurement fraud is a complex problem covering a range of schemes that are both numerous and diverse. Schemes can include corruption through bid rigging during the pre-contract stage through to false invoicing post-contract award, amongst others.

Corruption means bribes in the form of gifts or other advantages of various types. Corruption can occur at all stages of goods and services purchase, i.e. in the bidding phase, during the supplier selection, in the actual goods delivery stage and at payment. The best-known forms of fraud and corruption include:

- Purchase terms tailored for a specific supplier.
- Circumvention of the bidding process (bid rotation, bid suppression, creation of complementary and phantom bids, and/or disqualification of qualified applicants).
- Low-quality goods delivered instead of the originally contracted ones, incomplete contracts or improper billing.
- Invoicing schemes; the Organisation purchases and pays for goods and services which do not exist, are overpriced, or which the Organisation does not need at all. Fictitious (phantom or shell) companies, refunds into the offender's account and misuse of Organisation funds for an employee's private purposes are oft-used schemes.
- Fraud schemes involving conflicts of interest include purchase of overpriced goods/services from companies related to an employee of the Organisation or favouring of related companies within the bidding process.

Raising Orders

Where procurements are made through the I-Procurement system and operating processes, strong controls were found to be in place for a number of procurement fraud schemes such as false invoicing and overcharging and were found to be appropriate in mitigating the associated fraud risks. However, the December 2014 Financial Systems Assurance Audit identified that 43% of transactions were not subject to an order. Many of these transactions are not required to have an order by the Organisation and on that measure, 10% that required an order bypassed the I-Procurement system and did not have an order.

This bypass increases the Organisations exposure to fraud risk schemes such as false or duplicate invoicing, false payment authorisation, inappropriate purchasing, unauthorised purchasing and schemes involving supplier and purchaser collusion. The bypass weakens segregation of duty controls including approval and authorisation, weakens approved supplier controls and the system mandated 3 way match between ordering, goods receipt and invoices.

The overall effect is that reliance is then placed on unknown local systems for the recording of the order and receipt of goods and services.

Additionally, whilst not directly a fraud risk, the bypass results in a significantly more inefficient process, wasting resource that could be more effectively applied elsewhere.

Procurement Fraud Expertise

Like much of the public and private sector, the Organisation is vulnerable to large scale procurement fraud risk schemes such as bid rigging, market sharing and sale of bid information.

Bid-rigging agreements are notoriously difficult to detect as they are typically negotiated in secret in industries where collusion is common. A level of expertise and specialism is required and it can be necessary to look for clues such as unusual bidding or pricing patterns, or something that the supplier says or does. It is therefore important to be vigilant throughout the entire procurement process, as well as during preliminary market research.

The Organisation utilise Regional Procurement for large scale procurements over £50,000, however, discussions with the Regional Procurement Team established that whilst the team is experienced and CIPS qualified, it does not currently have any resource that has been professionally counter-fraud trained and thus may not have the knowledge and skills to effectively counter what is an extremely difficult fraud to identify and manage.

The National Fraud Authority: 2011 Procurement Fraud in the Public Sector report advises that Professional training is an important tool in strengthening a procurement official’s awareness of competition issues in public procurement. This has been recognised by the Chartered Institute of Procurement & Supply who as of August 2014 has made available the first E-Learning anti-Procurement Fraud training program to enable CIPS practitioners to more effectively identify and mitigate procurement fraud.

Efforts to fight bid rigging more effectively can be supported by collecting historical information on bidding behaviour, by constantly monitoring bidding activities, and by performing analyses on bid data. This would help Regional Procurement to identify problematic situations.

Additionally Professional counter-fraud training would also allow Regional Procurement to share their expertise both amongst themselves and also to the Organisations that they serve, potentially improving the control framework throughout all aspects of procurement.

Recommendation 2

The Organisation should assure itself that local processes in place are sufficient to manage the exposure to fraud risks, this assurance could be provided by Internal Audit.

Recommendation 3

Regional Procurement should make arrangements for existing resource to undertake appropriate counter-fraud training. Professional Counter-Fraud training would increase the effectiveness of the team in identifying and managing large scale procurement fraud risk schemes.

The counter-fraud trained resource should also be utilised to advise the supported organisations on effective practice in reducing the risk of fraud throughout the procurement process resulting a more efficient and effective control framework.

4.4 Payroll

Risk Exposure			Root causes		
Misappropriation of monetary assets			• Absence of reconciliation between system records and HR requests		
Probability	**Financial**	**Reputation**	**Operational**	**Legal**	**Rating**
Unlikely	Minor	Minor	Minor	Negligible	4 (5: 5)

Payroll fraud and error in the NHS is contributing to £7bn (7% of NHS annual budget at the time) being lost a year, according to a recent study*. The study considers fraudulent activity to be worth as much as £5bn, with a further £2bn could be lost through administrative mistakes – including those of paying staff, it is reasonable to assume that losses to the Organisation whilst not totalling such values, are proportionate to those found throughout the NHS.

There are three types of payroll fraud that organisations are commonly victim to:

1. **Ghost employee frauds**
   A ghost employee is someone recorded on the payroll system that does not work for the business. The ghost can be a real person that is placed into the system or a fictitious person invented by the fraudster.

2. **False wage claim frauds**
   False wage claim fraud is falsely adding extra hours or other relevant factors to wage information to increase remuneration. This fraud is done simply by altering time sheets sent for processing, the time recording system directly, or by any other factor like overtime payments.

3. **False expense reimbursement frauds**
   False expense reimbursement fraud is the making of improper claims for the reimbursement of business expenses. There are four major types of this fraud:
   - Mischaracterised expenses
   - Inflated expenses
   - False expenses
   - Multiple claims

The first two fraud types attack the payment system, whilst the third attacks the expense reimbursement systems.

Ghost Employees
The fraud risk assessment identified scope for improvement around controls to detect ghost employees. Currently all new employees are set-up by payroll following a request from HR. These setups are independently checked by a colleague to the paperwork received from HR, however, were an individual to set up a ghost employee and not submit it for checking then

there would not be anything to prompt a check. As recommended in the December 2014 Payroll audit report, via exception reporting a listing should be periodically generated from the payroll system of all newly created employees and these should be checked to supporting documentation.

Improper Changes to Pay

The assessment identified potential improvements to controls in respect of improper changes to pay. Currently changes are made to the Payroll system by the payroll team following a request from HR. These changes are then independently checked by a colleague to the request received from HR, however, were a payroll officer to make an improper change and not submit it for checking, there would not be anything to prompt a check. As recommended in the December 2014 Payroll audit report, via exception reporting a listing should be periodically generated from the payroll system of all pay amendments and these should be checked to supporting documentation.

RECOMMENDATIONS MADE PREVIOUSLY IN OTHER AUDITS

* *The Financial Cost of Healthcare Fraud 2014*

4.5 Compensation Claims

Risk Exposure			Root causes		
Misappropriation of monetary assets			• Absence of counter fraud process for compensation claims.		
Probability	**Financial**	**Reputation**	**Operational**	**Legal**	**Rating**
Probable	Minor	Minor	Negligible	Negligible	6 (5: 8)

Insurance fraud is when someone invents or exaggerates a claim. The Association of British Insurers estimates that fraud adds, on average, an extra £50 to the annual insurance bill for every UK policyholder. General insurers detected 118,500 cases of attempted claims fraud in 2013 totalling almost £1.3bn, an 18% increase in value compared to 2012. Fraud was most likely to be detected in liability insurance. This is why insurers invest at least £200 million each year to identify fraud.

Gallagher Bassett Compensation Recovery Unit performed an audit on Organisation processes around compensation claims. Their audit of 20 insurance claims raised the issue that the Organisation has no formal counter fraud process in place and that there was little visible evidence on files to suggest that fraud is being considered when dealing with compensation claims.

The Organisation is not seen to be giving due consideration to the fact that compensation claims received may be fraudulent and is therefore leaving itself exposed to fraudulent claims.

Gallagher Basset recommended that the Organisation develop an internal counter fraud process to ensure that all claims are screened for potential fraud and that this is recorded on the file.

RECOMMENDATION RAISED BY GALLAGHER BASSET

5. Recommendations

#	Recommendation	Category of Rec.	Management Action	Action Manager & Completion Date	Satisfactory Response (IA View)
1	The Organisation should adopt the fraud risk assessment and assign formal responsibility for its maintenance to a given individual / department. Periodic updating of the assessment should be undertaken in order to retain relevance through taking account of both the changing fraud and control environments and the evolving structure of the Organisation. The results of the fraud risk assessment should be used to help guide anti-fraud activity.	*Fundamental*	The Risk and Assurance Unit shall undertake a review of the related material in order to develop a clear understanding of the requirement, design an appropriate process for Fraud Risk Assessment including the associated resource requirement. An initial assessment was undertaken on the 13 August with Internal Audit. Residual risk scoring indicates an overall outcome of 83% green and 17% amber. Internal Audit cover most of the 17% criteria in their annual audit plan, this will be discussed with new Internal Auditors for future annual audit plans. Consideration will be given to dip sampling any gaps regarding the 17% amber, by the Risk and Assurance Unit and this will be built into the overall compliance activity calendar.	Risk & Assurance Manager 31December, 2015 Service Review Manager 31 March, 2016	Yes

#	Recommendation	Category of Rec.	Management Action	Action Manager & Completion Date	Satisfactory Response (IA View)
2	The Organisation should assure itself that local processes in place are sufficient to manage the exposure to fraud risks, this assurance could be provided by Internal Audit.	*Significant*	Internal Audit cover most of the 17% criteria in their annual audit plan, this will be discussed with new Internal Auditors for future year annual audit plans. Internal Audit will be asked to include Fraud Risk Assessments within each of their audit briefs/scopes.	Risk & Assurance Manager 31 December, 2015	Yes
3	Regional Procurement should make arrangements for existing resource to undertake appropriate counter-fraud training. Professional Counter-Fraud training would increase the effectiveness of the team in identifying and managing large scale procurement fraud risk schemes. The counter-fraud trained resource should also be utilised to advise the supported organisations on effective practice in reducing the risk of fraud throughout the procurement process resulting a more efficient and effective control framework.	*Significant*	By the 30th June 2015 The regional procurement manager will investigate training options specific to anti-procurement fraud and arrange appropriate staff to undertake training. Staff will have undertaken the appropriate training by 31 December 2015.	Chris Mottershaw MCIPS Director of Regional Procurement 30 June 2015	*Yes*

Classification of Recommendations	
Fundamental	Action is needed to address risks that could impact on the Organisation's ability to achieve its objectives. Action will typically be Organisation-wide and be necessary at the highest level. Other fundamental recommendations will be made in regard to potentially serious breaches of statutory obligations.
Significant	Action is needed to address risks that impact primarily on one major business area or to address lower risks on Organisation-wide basis.
Merits Attention	Action is advised to enhance control, remedy minor breaches of current controls or to improve efficiency.

Appendix 1

Appendix: Risk Assessment Criteria

The risks in the Fraud Risk Assessment have been assessed using the North Yorkshire Police Strategic Risk Matrix criteria:

Probability	Nil	< 20% Highly Improbable	20% - 40% Unlikely	40% - 60% Probable	> 60% Highly Probable
Impact Categories	**Nil**	**Negligible**	**Minor**	**Significant**	**Severe**
Financial (£) - Default - Mandatory	Nil	0 - <100k Financial impact less than £100k	100k - <=250k Financial impact between £100k and £250k	250k - <=2.5m Financial impact between £250k and £2.5m	>2.5m Financial impact greater than £2.5m
Reputation	Nil	• Negligible adverse publicity. • Minimal impact upon public perception	• Localised adverse publicity. • Minor/transient impact upon public perception of Organisation or PCC	• Criticism at local level. • Lasting impact upon public perception of Organisation or PCC	• Intense national media. • Criticism at national level
Operational	Nil	Negligible impact upon ability to deliver service and meet Organisation targets	Minor impact upon ability to deliver service and meet Organisation targets	Significant impact upon ability to deliver service and meet Organisation targets	Severe impact upon ability to deliver service and meet Organisation targets
Legal/Compliance	Nil	Negligible prospect of legal challenge	Minor/Transient prospect of legal challenge	• Serious non-compliance. • Litigation/challenge.	National legal issue.

On the outcome of the assessment against the North Yorkshire Police Strategic Risk Matrix, the risks have then been categorised as High, Medium or Low based on the Organisation Risk Appetite as seen below:

Likelihood						
Highly Probable	4	0	4	8	12	16
Probable	3	0	3	6	9	12
Unlikely	2	0	2	4	6	8
Highly Improbable	1	0	1	2	3	4
Nil	0	0	0	0	0	0
		0	1	2	3	4
	Impact	Nil	Negligible	Minor	Significant	Severe

Appendix 2

Organisational Fraud – Context

The Audit Commission Protecting the Public Purse 2014 report (PPP2014) defines fraud as:

> *An intentional false representation, including failure to declare information or abuse of position that is carried out to make gain, cause loss or expose another to the risk of loss.*

A University of Leicester study in 2003 found that from a survey of 2000 people, 70% admitted they would commit fraud if they knew they could get away with it, this suggests that fraud (or an individual's potential to commit fraud) is far more prevalent than people realise.

Organisations are subject to fraud from both outside and inside the organisation and are regularly the victims of fraud schemes only possible through collusion between both. Employees colluding can bypass controls and thus enable the misappropriation of much greater amounts.

PPP2014 stated that cases of detected Procurement Fraud had fallen by 37% from 2012/13 to 2013/14, however, the average value of each detected fraud case has risen by 270% from £9,360 to £34,646. Initially it appears promising that there has been a fall in the number of detected fraud cases, however, PPP2014 indicates that there is a direct correlation between reduced fraud detection resource, the resultant weakening of controls as staffing numbers and expertise are lost and the consequential resulting failure to detect fraud.

The Audit Commission state that in their experience, the more organisations look for fraud, and follow good practice, the more they will find. Increasing levels of detection may therefore be a positive sign that organisations take fraud seriously, rather than evidence of weak counter-fraud controls.

PPP2014 states that Investigating fraud can be expensive. Additional costs may be incurred in prosecuting fraudsters and in attempting to recover money, which is not always successful. It is usually more cost-effective to prevent fraud than to take action afterwards.

The True Cost of Insider Fraud (Information from CIFAS – The UK's Fraud Prevention Service)

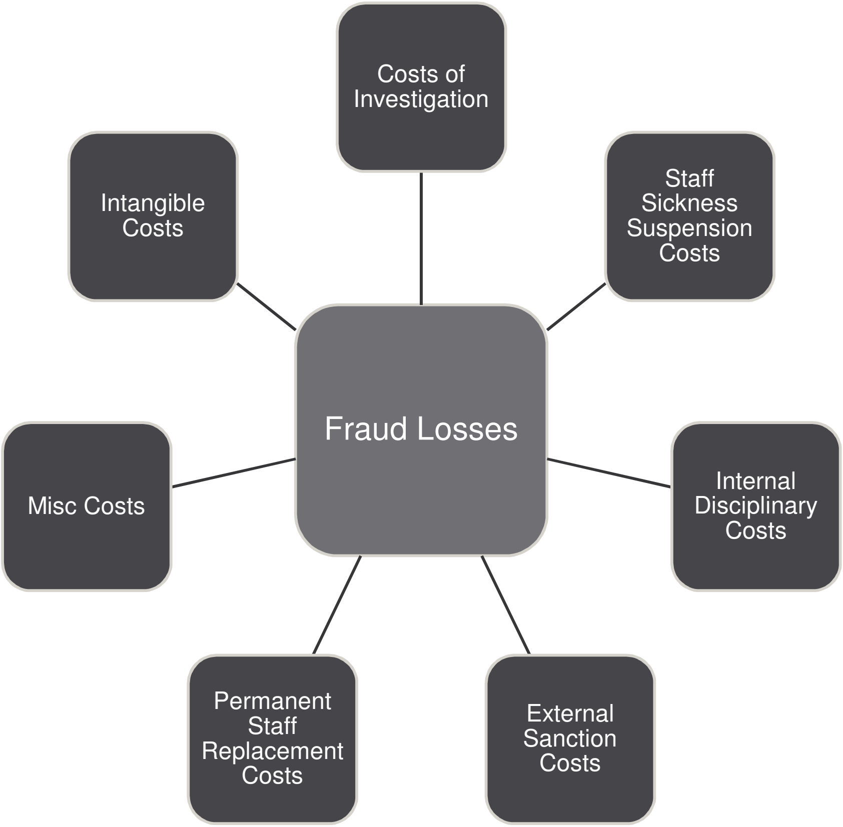
The University of Portsmouth: Centre for Counter Fraud Studies analysis of numerous occurrences of internal fraud identified how much greater the total cost of Fraud is compared with the initial loss:

- Smaller frauds result in a disproportionate increase in the total cost. Frauds under £25,000 incurred costs averaging a 265% increase to the initial loss, consequently a £300 fraud loss will incur, on average, a £795 associated cost and a final cost of £1,095; while, a £10,000 fraud could cost over £36,000.

- 61% of costs incurred by the public sector were due to sickness leave or absence taken by the person under investigation. Consequently, for the above £300 fraud example, the final bill to the public sector was actually £1,560, £767 of that final bill equates to sick leave or absence costs: two and a half times greater than the initial loss.
- Of the intangible costs, the impact upon the morale of the fraudster's former colleagues was deemed by research participants to be the greatest threat, while the impact upon the financial strength of an organisation the least threatening.

The costs associated with internal fraud therefore far exceed the amount initially lost and are unavoidable once internal fraud has been identified. The associated internal fraud costs diversity can be seen in ***Figure 2***:

Figure 2


Costs of Investigation
Staff Sickness Suspension Costs
Internal Disciplinary Costs
External Sanction Costs
Permanent Staff Replacement Costs
Misc Costs
Intangible Costs
Fraud Losses

On this basis it may be financially preferable to not identify fraud and therefore incur the associated costs, however, leaders in the public sector are expected to and have a responsibility to protect public funds. Therefore, as supported by the findings from the both the CIFAS report and PPP2014, investment in prevention can be preferable to paying out the additional and escalating costs incurred as a result of fraud.

Appendix 3

Strategic Aims: Managing the risk of Fraud and Corruption

The CIPFA code of practice: Managing the risk of fraud and corruption states:

> *Leaders of public services organisations have a responsibility to embed effective standards for countering fraud and corruption in their organisations. This supports good governance, demonstrates effective financial stewardship and strong public financial management.*

A comprehensive fraud prevention strategy combined with appropriate HR procedures should be the cornerstone of the Organisations work: helping to instil a zero tolerance attitude to fraud, ensures staff have neither the motivation nor the opportunity to commit fraud from the inside. Should a case arise, however, further losses can be restricted if the Organisation acts swiftly and decisively, thus restricting associated costs.

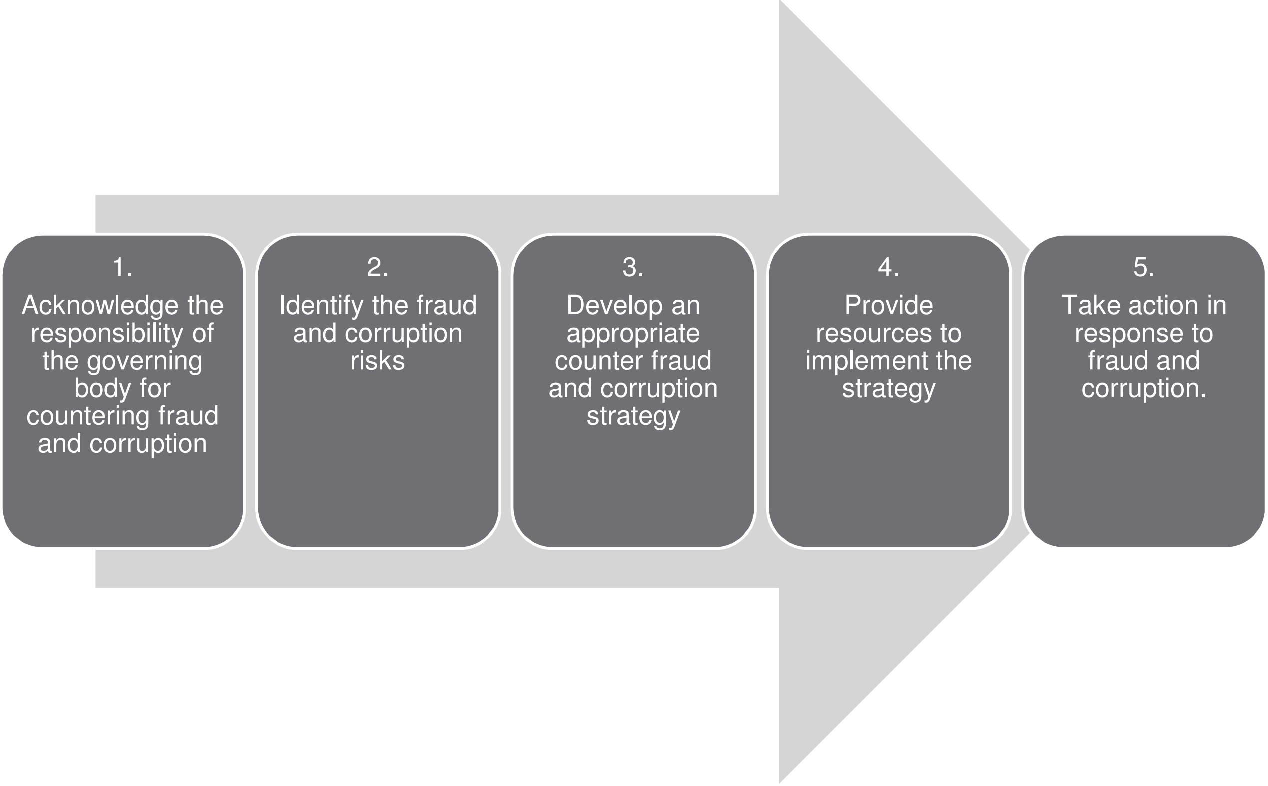
An effective strategic approach to understanding and managing the risks of fraud and corruption:

- Improves corporate governance through a sound assessment of the Organisations risks, fraud risks should be managed in the same manner as other Organisational risks i.e. be approached systematically at both Organisational and operational levels.
- Assists in developing appropriate mitigating controls that target proportionate pressure at all areas of the problem.
- Facilitates a cost effective approach by focusing limited resource on areas of greatest need. A strategy can also assist in providing a robust and rational basis on which to bid for resource to tackle fraud.
- Can be useful as a mechanism to communicate the Organisations aims and expectations of what is expected from staff and other stakeholders.
- Can be publicised to deter fraudsters, both internal and external who will recognise that the Organisation is not an easy target and that the risks outweigh rewards.

Effectively managing the risk of fraud and corruption

The process, covered through 5 Key Principles, to effectively managing the risk of fraud and corruption is detailed in the CIPFA Code of Practice 2014. See ***Figure 3.*** Further detail on each of the principles and how they can be applied to the Organisation follows below.

Figure 3 – The 5 Key Principles



1.
Acknowledge the responsibility of the governing body for countering fraud and corruption
2.
Identify the fraud and corruption risks
3.
Develop an appropriate counter fraud and corruption strategy
4.
Provide resources to implement the strategy
5.
Take action in response to fraud and corruption.

Acknowledge the responsibility of the governing body for countering fraud and corruption

Organisation leadership should acknowledge their responsibility for ensuring that fraud and corruption risks are appropriately managed throughout the Organisation.

In order to achieve this:

- The Organisation leadership team should acknowledge the threat of fraud and corruption and the harm it can cause to the Organisation, its aims, objectives and to the community it serves.
- The Organisation leadership team should acknowledge the importance of establishing a culture that is resilient to the threats of fraud and corruption and aligns to the principles of good governance.

- The Organisation Leadership Team should acknowledge its responsibility for ensuring the appropriate management of Organisation fraud and corruption risks and its accountability for the actions it takes through its governance reports.
- The Leadership Team should set a specific goal of ensuring and maintaining the Organisations resilience to fraud and corruption and explore opportunities for financial savings achieved through enhanced fraud detection and prevention.

Theft and Fraud Policy and Adoption of the Code of Ethics

The Organisation opposes the loss of public funds allocated for policing to fraud and corruption through its Anti-Fraud, Anti-Corruption and Confidential Reporting policy and through adoption of the Code of Ethics (A Code of Practice for the Principles and Standards of Professional Behaviour for the Policing Profession of England and Wales.)

Identify the fraud and corruption risks – The Fraud Risk Assessment

The identification of fraud risk is essential to understanding specific risk exposures, the changing nature of the fraud environment and the potential consequences to the Organisation and the community it serves.

In order to achieve this:

- The Organisation should adopt and maintain the fraud risk assessment produced by Internal Audit.
- Fraud risks should be routinely considered as part of the Organisation risk management arrangements.
- The Organisation should identify the risks of corruption and the importance of behaving with integrity in its governance framework.
- The Organisation should use published estimates of fraud loss, and where possible its own measurement exercises to improve its evaluation of Organisation fraud risk exposures.
- The Organisation should evaluate the harm to its aims, objectives and the community it serves that different fraud risks can cause.

Develop a strategy

The Organisation should have a counter fraud strategy setting out its approach to managing its risks and defining responsibilities for action.

In order to achieve this:

- The Leadership Team should formally adopt a counter fraud and corruption strategy to address the identified risks and align with the Organisation’s acknowledged responsibilities and goals.

- The strategy should include the Organisation use of joint working or partnership approaches to managing its risks, where appropriate.
- The strategy should include both proactive and responsive approaches best suited to Organisation fraud and corruption risks. Proactive and responsive elements of a good practice fraud risk management response are below:

Proactive

- Develop a counter-fraud culture to increase resilience to fraud.
- Prevent fraud through implementing appropriate and robust internal controls and security measures.
- Data matching to validate data.
- Deter fraud attempts through publication of the Organisation anti-fraud and corruption stance, naming and shaming and actions taken against fraudsters.

Responsive

- Detect fraud through analysis of data and intelligence.
- Effective whistleblowing arrangements.
- Investigate fraud referrals.
- Apply sanctions, such as internal disciplinary, regulatory and criminal proceedings.
- Seek redress, such as recovery of assets and money where possible.

- The strategy should include clear identification of responsibility and accountability for its delivery and providing oversight.

Provide resources

The Organisation should make arrangements for appropriate resources to support the counter fraud strategy.

In order to achieve this:

- Perform an annual assessment of whether resource invested to counter fraud and corruption is proportionate for the level of risk.
- Utilise an appropriate mix of experienced and skilled staff, including access to counter fraud staff with professional accreditation.
- Grants counter fraud staff unhindered access to employees, information and other resources as required for investigation purposes.
- Have protocols in place to facilitate joint working and data and intelligence sharing to support counter fraud activity.

Take action

The Organisation should put in place policies and procedures to support the counter fraud and corruption strategy and take action to prevent, detect and investigate fraud.

In order to achieve this:

- The Organisation should introduce a policy framework that supports the implementation of the counter fraud strategy, policies should, at the least, include:
  - Counter fraud policy
  - Whistleblowing policy
  - Anti-money laundering policy
  - Anti-bribery policy
  - Anti-corruption policy
  - Gifts and hospitality policy and register
  - Pecuniary interest and conflicts of interest policies and register
  - Codes of conduct and ethics
  - Information security policy
  - Cyber security policy.

- Plans and operations should be aligned to the strategy and contribute to the achievement of the Organisation goal of maintaining resilience to fraud and corruption.
- Make effective use of national or sector initiatives for detection and prevention of fraud, such as data matching or intelligence sharing.
- Provide for independent assurance over fraud risk management, strategy and activities.
- There should be a report to the Leadership Team and Audit Committee at least annually on performance against the counter fraud strategy and its effectiveness from the designated lead person(s) for the strategy. Conclusions should be featured in the Organisation annual governance report.

Scoring Methodology / Example

Appendix 4

Fictitious (or ghost) employees on the payroll.

The fraud risk scheme is a payroll risk and relates to the input of ghost employees into the payroll system as a means of directing payment to the fraudster.

In order to obtain the **Risk Score** two factors are considered, these are **Likelihood** and **Impact**. The Risk Score is the multiplication of the Impact by the Likelihood. The category of risk that the score then relates to i.e. High, Medium or Low is determined by the Force risk appetite as seen at Appendix 1.

	Inherent	**Residual**
Likelihood	Probable (3)	Unlikely (2)
Impact	Significant (3)	Significant (3)
Risk Score	(3 x 3) = **9**	(2 x 3) = **6**

Inherent Risk

This is the risk that the Organisation is exposed to when compensating controls or other factors are not considered e.g.:

- No vetting of personnel,
- Unrestricted access to the payroll system,
- No verification of employee setups for legitimacy,
- No exception reporting to identify all new employee set-ups
- No budget and transaction monitoring,
- No limitations on transaction value.

Inherent Likelihood (3)

In the absence of controls or compensating factors it was assessed as probable that employees within the force would utilise the ghost employee scheme in order to obtain undue payment.

Inherent Impact (3)

In the absence of controls or compensating factors the impact was assessed as being significant.

- Financially the cost implications could conceivably exceed £250k or higher.
- Criticism would occur at local level and would have a lasting impact upon public perception of the Organisation and OPCC, particularly considering the current National austerity drive and media attention on Police resource.

Inherent Risk Score

The score was worked out as 3 x 3 = 9, which using the Organisations risk appetite criteria works out as a Medium risk.

Residual Risk

This is the risk that remains once actual controls and mitigating factors are taken into account.

Scoring Methodology / Example

Appendix 4

Actual Controls

The assessment utilised information obtained from the 2014 Financial Systems audit to determine what actual controls the Organisation has in place, these were established as being:

- Access to the payroll system is restricted – Only 3 people in Payroll can set-up new users and this is split alphabetically.
- Payroll do not input new starters onto the payroll system without appropriate authorisation and sufficient signatures from the employee on the required forms.
- Forms are verified as being dated on or after the contracted start date.
- If the authorisation or date parameter requirements are not met, then payroll query the forms and return to HR.
- All New Starter Inputs onto the payroll system are 100% independently checked by a member of payroll to supporting documentation. However, this is dependent on the inputter making the checker aware that the entry requires checking. A fraudster would be unlikely to request that a ghost employee be checked.
- Centralised budget monitoring.

Weaknesses

- Budget monitoring is centralised, in respect of the ghost employee risk, this is less effective than local budget monitoring. Local expertise is not utilised to determine whether those being paid in an area reside there, however, this is mitigated to an extent by the relatively small size of the Organisation.
- Exception reporting of all new starters is not currently performed. A payroll report could be run from the system listing all new starters and these could be verified to supporting HR documentation, this would be a more efficient and effective control than the current 100% check.

Residual Likelihood (2)

The actual controls reduce the likelihood of this risk occurring to unlikely from probable, however, due to the weaknesses identified in the actual controls the likelihood cannot be reduced further as there a couple of vulnerabilities in the process.

Residual Impact (3)

The financial impact is likely to reduce from significant to negligible or at most minor, however, the reputational impact remains significant, so there is no change in the impact level.

Residual Risk Score

The score was assessed as 2 x 3 = 6, which using the force risk appetite criteria works out as a low risk.