Risks, controls and actions - Fraud

as at 17.02.14

Risk Identified	Potential Consequences	Impact	Risk Rating	Control Measure	Final Risk Rating	Further Action Required
Fraud Awareness						Risk Count: 34
Abuse of email	Misappropriation of Council time. Reputation damage.	a	E	Acceptable use policy signed by staff Code of Conduct for Officers and Members Information Security Policies Mail meter reports sent to Heads of Service	7	Roll out of elearning training module for misuse of time and resources Roll out E Learning Training Module Regular review of mailmeter reports
Postal voting fraud	Elections become null and void. Financial implications. Reputation damage. Resource issues.	a	E	Registrations and applications vetted Review of process Training of staff for postal opening Electoral Commission checks undertaken	6	
Theft of income	Misappropriation of funds. Criminal investigation. Reputation damage.	a	E	Issue of receipts for income Two people open post CRB checks undertaken References taken for new employees Regular independent reconciliation of income taken to income expected Regular banking and banking checks	5	Consider roll out of CRB to other depts.

Risk Identified	Potential Consequences	Impact	Risk Rating	Control Measure	Final Risk Rating	Further Action Required
Fraud Awareness						Risk Count: 34
				Compliance with cash handling instructions and financial regulations Income collection systems - separation of duties		
Fraudulent benefit claims	Misappropriation of funds. Criminal investigation. Reputation damage.	a	E	Verification by benefit assessors Checks of details by verification framework officers Benefit investigators Fraud awareness training to all staff National Fraud Initiative (NFI)	5	Review resource allocation in respect of fraud investigation
Failure to recover money	Misappropriation of funds. Criminal investigation. Reputation damage.	a	E	Laid down procedures Exception reporting Debtors system - separation of responsibilities Recovery procedures exception reporting	5	Process to be looked at for BACS Regular review of systems Review of trade refuse rounds
Fraudulent letting or extension of contracts	Criminal investigation. Reputational damage. Possible breach of OJEC rules. Third Party involvement.	a	E	Central register of contracts is maintained by the Procurement Officer Code of Conduct for Officers and Members	3	Remind staff to involve procurement officer when letting or extending contracts

Risk Identified	Potential Consequences	Impact	Risk Rating	Control Measure	Final Risk Rating	Further Action Required
Fraud Awareness						Risk Count: 34
				Procurement Officer in post Procurement toolkit IDeA training Standing Orders Financial Regulations Final Account Audit undertaken Procurement Briefings Anti-Fraud and Anti-Corruption Policy		
Unauthorised access to computer systems for fraudulent use	Loss of data. Corruption of data. Financial gain. Reputational damage. Failure to work. Loss of Government Connects authorisation. Criminal investigation.	a	E	Network security policy Training - on computer security Access controls Information Security Policies	3	Elearning tool to refresh on annual basis Access controls audited annually
Corruption in sale of land	Abuse of position. Abuse of public office. Criminal investigation. Financial implications. Officers open to bribery & corruption.	a	E	Valuations of land for sale Financial Regulations Standing Orders Capital Asset Accountant Capital Asset Working Group Cabinet approval of sale of land Robust screening process	3	Consider CRB checks for Assets staff

Risk Identified	Potential Consequences	Impact	Risk Rating	Control Measure	Final Risk Rating	Further Action Required
Fraud Awareness						Risk Count: 34
Falsification of performance indicators	Public perception reduced. Reputation damage. Inaccurate benchmarking measurements used.	a	E	Independent check of performance indicator statistics / data Password protected performance system	3	
Fraudulent invoices or claims from contractors	Misappropriation of funds. Criminal offences. Reputational damage.	a	E	Agresso purchase order processing Training for budget holders Financial Regulations Creditors system - separation of duties / responsibilities Budget monitoring Contract monitoring Annual core system audit National Fraud Initiative (NFI) Large cheques have to be signed individually Regular software checks done re valid list of suppliers.	3	Software check done annually to look at internal system
Fraudulent Bank Notes	Loss of income to the Council	1	7	Scan Coin Machines have detection facilities in place UV Marker pens in use	7	On Line Training - via SafeVoice On Line Training
Fraudulent use of Corporate Credit Cards	Misappropriation of funds. Criminal investigation. Reputation damage.	a	E	Training - on Corporate Credit Card system	4	

Risk Identified	Potential Consequences	Impact	Risk Rating	Control Measure	Final Risk Rating	Further Action Required
Fraud Awareness						Risk Count: 34
				Compliance with Credit Card procedures Review of policies Monthly review of transactions and suppliers Responsibilities formally allocated and agreed by cardholder Credit Card - regular review of procedures by Internal Audit Credit Card - separation of duties £5,000 limit per month per corporate credit card		
Fraudulent use of investment money	Insurance implications. Increase cost in insurance premium. Abuse in position. Abuse of public office. Financial implications. Reputation damage.	a	E	Annual audit of treasury management Treasury Management meetings Fidelity guarantee insurance for designated officers Treasury Management - statutory / professional guidance Use of Broker and Treasury Management advisors	2	

Risk Identified	Potential Consequences	Impact	Risk Rating	Control Measure	Final Risk Rating	Further Action Required
Fraud Awareness						Risk Count: 34
				Carry out periodic reconciliations Separation of responsibilities for investments		
Fraudulently using external funding	Reputation damage. Financial assistance would be cut off. Budgetary implications. Failure to deliver projects. Service delivery reduced.	a	E	Budget monitoring External funding - separation of duties Newcastle Borough Council acts on lessons learnt Financial Regulations Standing Orders Independent verification of grant conditions Audit undertaken	2	Ensure staff app;y the Third Sector Commissioning Framework principles to grant funding Train staff in how to pay out grants Train staff in correct external funding / grant procedures and processes for claiming grants
Theft or misuse of the Authority's information	Failure to work. Loss of Government Connects authorisation. Loss of data. Corruption of data. Financial gain. Reputational damage.	a	E	Clear desk policy Confidential information locked away Confidentiality clauses Encrypted memory sticks Access controls Saving data to servers Firewalls Information Security Policies Managing Information Risks risk assessment	2	Work to meet requirements of PCI Training to be organised in data protection, copyright etc Control procedures to be written up in relation to visitors and meetings etc Strong 2 factor authentication Third party contracts in place for supply of OS data

Risk Identified	Potential Consequences	Impact	Risk Rating	Control Measure	Final Risk Rating	Further Action Required
Fraud Awareness						Risk Count: 34
				Information Security Working Group		Information Security Briefings
				Connected to Government Secure Intranet		Information Security Briefings
				Inspire directive for sharing of data across EU		
				Metadata to ISO standards. Use of data for application.		
Fraudulent use of council vehicles	Breach of insurance cover. Criminal investigation. Reputation damage. Financial implications.	a	E	Vehicle logs	2	
				Staff awareness of insurance implications		
				Driving at work policy		
Inappropriate receipts of gifts / hospitality	Officers open to bribery and corruption. Reputational damage.	a	E	Code of Conduct for Officers and Members	1	To ensure that the Gifts and Hospitality Policy is Reviewed
				Manager approval		
				Register of Interests		
				Audit undertaken		
				Staff informed of process		
				Annual reminders		
Theft or sale of official stocks / equipment	Misappropriation of funds. Criminal investigation. Reputation damage. Loss of data. Corruption of data. Financial gain. Failure to work. Loss of Government Connects authorisation.	a	E	Regular independent checks of stocks / equipment across the council	1	ICT to produce work programme to security mark all ICT equipment
				Stock records maintained across all service areas within the council		

Risk Identified	Potential Consequences	Impact	Risk Rating	Control Measure	Final Risk Rating	Further Action Required
Fraud Awareness						Risk Count: 34
				Inventory of all ICT items (numbered) PCs are tagged/marked Annual inventory checks Physical security		
Misappropriation of funds	Abuse of position. Abuse of public office.	a	E	Minimising cash payments by debit card and direct payment methods Regular independent reconciliations of funds Cash secured Cash and income collection - separation of duties Budget monitoring Whistleblowing policy Financial Regulations	1	Documented clear work procedures to be produced
Fraudulent payments for personal gain	Misappropriation of funds. Criminal investigation. Reputation damage.	a	E	Independent reconciliations Approval process Budget monitoring	1	
Fraudulent car loans	Misappropriation of funds. Criminal investigation. Reputation damage.	d	M	Clear procedures for car loan applications Car Loans - separation of duties Affordability check	1	

Risk Identified	Potential Consequences	Impact	Risk Rating	Control Measure	Final Risk Rating	Further Action Required
Fraud Awareness						Risk Count: 34
Money laundering	Criminal investigation. Reputation damage. Financial implications.	a	H	Money Laundering - statutory / professional guidance Audit review procedures and recommendations made Cashiers audit	1	Money laundering training to be rolled out to staff
Agency staff claiming hours not worked	Misappropriation of funds. Criminal investigation. Reputation damage.	c	H	Line manager checks hours worked Use of timekeeper system HR involvement	1	
Theft from vulnerable people	Misappropriation of funds. Criminal investigation. Reputation damage. Abuse of position. Abuse of public office.	b	H	CRB checks undertaken Code of Conduct for Officers and Members Receipts given for valuables Proper and safe handover procedures	1	
Theft of cash in transit	Misappropriation of funds. Criminal investigation. Reputation damage.	c	H	Reducing cash transactions Audit review procedures and recommendations made Cash in transit - staff training Varying routes and drop off points, times etc Cybertrack phone issued to relevant staff	1	Produce insurance risk assessment for process

Risk Identified	Potential Consequences	Impact	Risk Rating	Control Measure	Final Risk Rating	Further Action Required
Fraud Awareness						Risk Count: 34
				Handled by securicor / G4S		
Subletting of NBC properties	Abuse of position. Abuse of public office. Criminal investigation.	c	H	Accurate details of premises to let Clear instructions to staff Reconciliation of income Management checks of properties	1	
Abuse of telephones	Misappropriation of funds. Criminal investigation. Reputation damage. Misappropriation of Council time.	e	M	Mobile phone provider System in place for identifying personal calls and text messages Telephone usage policy (corporate) in place Register of Interests Regular telephone reports to management	1	Regular reports to management to be produced
Abuse of postage system	Misappropriation of funds. Criminal investigation. Reputation damage.	e	M	Management check of postage costs Budget monitoring Protocols set for handling of post	1	
Abuse of internet	Misappropriation of Council time. Reputation damage.	d	H	Acceptable use policy signed by staff Code of Conduct for Officers and Members Websense categories for certain web pages	1	Internet reports to be produced

Risk Identified	Potential Consequences	Impact	Risk Rating	Control Measure	Final Risk Rating	Further Action Required
Fraud Awareness						Risk Count: 34
Payments to ghost employees	Misappropriation of funds. Criminal investigation. Reputation damage.	b	H	Budget monitoring Payroll - Separation of duties Review of payroll processes Review of payroll system Recruitment policy and process Audit undertaken NFI checks completed annually	1	Implementing recommendations of HR audit - separation of duties
Fraudulently trading for personal gain	Misappropriation of funds. Criminal investigation. Reputation damage. Abuse of position. Abuse of public office.	a	E	Code of Conduct for Officers and Members National Fraud Initiative (NFI) Register of Interests Checks by management	1	Annual Reminer to staff regarding registering of outside interests. Annual Reminer to staff regarding registering of outside interests.
HR policies do not deter fraudulent behaviour	Insurance implications. Financial implications. Criminal investigation. Reputation damage.	b	E	Review of policies Disciplinary process Relevant stakeholders involved in review of processes Anti-Fraud and Anti-Corruption Policy Whistleblowing policy Managers Guide on Fraud Related policies in place	1	

Risk Identified	Potential Consequences	Impact	Risk Rating	Control Measure	Final Risk Rating	Further Action Required
Fraud Awareness						Risk Count: 34
Fraudulent job application forms	Inappropriate appointment. Security implications. Insurance implications. Financial implications. Criminal investigation. Reputation damage.	b	E	Obtain evidence of qualifications Obtain references HR involvement Recruitment policy and process Identity checks carried out	1	New policy linked to GCSX
Fraudulent non attendance at work	Abuse of contract. Abuse of public office. Abuse of position.	c	H	Checks of time by management Reconciliation of leave Compliance with management of attendance policy for sickness Review of management of attendance policy Audit of management of attendance Occupational Health to assist return to work Whistleblowing policy	1	