Risks, controls and actions - Fraud

as at 25/03/13

Risk Identified	Description	Potential Consequences	Control Measure	Description	Final Impact	Final Likelihood	Final Risk Rating	Further Action Required	Target Date	Owner
Fraud Awareness										Risk Count: 34
Abuse of email	Staff using email for personal use or sending inappropriate email	Misappropriation of Council time. Reputation damage.	Acceptable use policy signed by staff	Acceptable use policy signed by staff	1	3	7	Roll out of elearning training module for misuse of time and resources	31/03/13	Dodd, Liz (Audit Manager)
			Code of Conduct for Officers and Members	Email policy. Software blocking of certain words & sites.				Roll out E Learning Training Module	27/09/13	Dodd, Liz (Audit Manager)
			Information Security Policies	The Authority has a suite of 10 Information Security Policies based on professional guidance and best practice to ensure compliance with BS7799 or ISO equivalent.				Regular review of mailmeter reports	31/03/10	Dodd, Liz (Audit Manager)
			Mail meter reports sent to Heads of Service	Mail meter reports sent to Heads of Service						
Postal voting fraud	Voting fraud for elections	Elections become null and void. Financial implications. Reputation damage. Resource issues.	Registrations and applications vetted	More than 5 postal votes sent to an individual address are vetted and scanned into a signature recognition process	3	2	6			
			Review of process	Review of process						
			Training of staff for postal opening	Staff are trained to deal with suspected cased of impersonation, and to follow the advice of the electoral commission in taking appropriate measures						
			Electoral Commission checks undertaken	Electoral Commission check applications downloaded from their website - they track the computers and numbers of applications printed						
Theft of income	Theft of income generally, from all income streams	Misappropriation of funds. Criminal investigation. Reputation damage.	Issue of receipts for income	Issue of receipts for income	2	2	5	Consider roll out of CRB to other depts.	31/03/10	Durrant, Richard (Head of Human Resources)
			Two people open post	Two people open post						
			CRB checks undertaken	Checks for all new staff and then every three years - cost £32 - £36.						
			References taken for new employees	References taken for new employees						
			Regular independent reconciliation of income taken to income expected	Reconciling of income anticipated to income received						
			Regular banking and banking checks	Regular banking of income to prevent a build up of cash. Bulk checks of cash prior to banking independent check of bankings						

Fraud Awareness

Risk Count: 34

Risk Identified	Description	Potential Consequences	Control Measure	Description	Final Impact	Final Likelihood	Final Risk Rating	Further Action Required	Target Date	Owner
			Compliance with cash handling instructions and financial regulations	Training in cash handling instructions issued to staff. Financial regulations detailing council procedures						
			Income collection systems - separation of duties	There is separation of duties and responsibilities in all income collection systems						
Fraudulent benefit claims	Fraudulent benefit claims for housing and council tax benefit. Fraudulent benefit claims by NBC staff	Misappropriation of funds. Criminal investigation. Reputation damage.	Verification by benefit assessors	Verification by benefit assessors in line with guidelines	2	2	5	Review resource allocation in respect of fraud investigation	31/03/13	Baker, Dave (Head of Revenues & Benefits)
			Checks of details by verification framework officers	Checks of details by verification framework officers						
			Benefit investigators	A trained benefit investigator deals with fraud in Benefits. They link directly with DWP.						
			Fraud awareness training to all staff	Fraud awareness training to all staff						
			National Fraud Initiative (NFI)	The Authority participates in the National Fraud Initiative e.g benefit claim matches are identified and investigated, cheques are security printed to comply with APACS standard. A copy also goes to Payroll.						
Failure to recover money	Failure to recover money due to suppressing debtor or equivalent accounts	Misappropriation of funds. Criminal investigation. Reputation damage.	Laid down procedures	Laid down procedures for suppression of recovery action	2	2	5	Process to be looked at for BACS	31/05/13	Baker, Dave (Head of Revenues & Benefits)
			Exception reporting	Duplicate payment schedule identifies any cheque numbers that have already been presented				Regular review of systems Review of trade refuse rounds	31/12/09 31/03/10	Baker, Dave (Head of Revenues & Benefits) Tait, Roger (Head of Operations)
			Debtors system - separation of responsibilities	Separation of responsibilities for debtor accounts						
			Recovery procedures exception reporting	Recovery procedures exception reporting						
Fraudulent letting or extension of contracts	Fraudulent letting or extension of Council contracts due to collusion or corruption	Criminal investigation. Reputational damage. Possible breach of OJEC rules. Third Party involvement.	Central register of contracts is maintained by the Procurement Officer	Procurement professionals being involved in all major contract letting who work to a strict code of ethics	3	1	3	Remind staff to involve procurement officer when letting or extending contracts	31/12/09	Sowerby, Simon (Business Improvement Manager)
			Code of Conduct for Officers and Members	Email policy. Software blocking of certain words & sites.						
			Procurement Officer in post	Procurement Officer in post						
			Procurement toolkit	Procurement toolkit in place for staff to utilise with assistance from Procurement Officer						
			IDeA training	IDeA training						

Fraud Awareness

Risk Count: 34

Risk Identified	Description	Potential Consequences	Control Measure	Description	Final Impact	Final Likelihood	Final Risk Rating	Further Action Required	Target Date	Owner
			Standing Orders	Standing Orders in respect of contracts						
			Financial Regulations	Compliance with Financial Regulations						
			Final Account Audit undertaken	Internal audit to audit contracts as per all financial regulations						
			Procurement Briefings	Breifing session are delivered to all staff have a responsibility for any procurement matters						
			Anti-Fraud and Anti-Corruption Policy	Anti-Fraud and Anti-Corruption Policy						
Unauthorised access to computer systems for fraudulent use	Staff can gain inappropriate access to computer systems and alter data for personal gain	Loss of data. Corruption of data. Financial gain. Reputational damage. Failure to work. Loss of Government Connects authorisation. Criminal investigation.	Network security policy	Network security policy owned by IT. This covers overall access.	3	1	3	Elearning tool to refresh on annual basis Access controls audited annually	31/05/10 31/12/09	Dodd, Liz (Audit Manager) Dodd, Liz (Audit Manager)
			Training - on computer security	Training for users on how to avoid others obtaining unauthorised access - turning off PC's, password protected screensavers, complex password protection, access control.						
			Access controls	Controls and passwords on systems						
			Information Security Policies	The Authority has a suite of 10 Information Security Policies based on professional guidance and best practice to ensure compliance with BS7799 or ISO equivalent.						
Corruption in sale of land	Receiving personal gain for sale of land	Abuse of position. Abuse of public office. Criminal investigation. Financial implications. Officers open to bribery & corruption.	Valuations of land for sale	Valuations of land for sale	3	1	3	Consider CRB checks for Assets staff	31/03/10	Durrant, Richard (Head of Human Resources)
			Financial Regulations	Compliance with Financial Regulations						
			Standing Orders	Standing Orders in respect of contracts						
			Capital Asset Accountant	Capital Asset Accountant						
			Capital Asset Working Group	Capital Asset Working Group						
			Cabinet approval of sale of land	Management / member approval of sale of land						
			Robust screening process	Robust screening process						
Falsification of performance indicators	Incorrect or manipulated data is used to produce performance indicators	Public perception reduced. Reputation damage. Inaccurate benchmarking measurements used.	Independent check of performance indicator statistics / data	Independent check of performance indicator statistics / data (data auditing)	3	1	3			

Fraud Awareness

Risk Count: 34

Risk Identified	Description	Potential Consequences	Control Measure	Description	Final Impact	Final Likelihood	Final Risk Rating	Further Action Required	Target Date	Owner
			Password protected performance system	CorVu system in place that is protected Corvu system no longer used by the authority. Spreadsheets are now maintained by the Business Improvement Officer (Procurement & Performance)						
Fraudulent invoices or claims from contractors	Fraudulent invoices paid by the Authority	Misappropriation of funds. Criminal offences. Reputational damage.	Agresso purchase order processing	Allowing approval from manager up front.	3	1	3	Software check done annually to look at internal system	31/12/09	Hilton, Jeanette (Head of Customer & ICT Services)
			Training for budget holders	Training for budget holders						
			Financial Regulations	Compliance with Financial Regulations						
			Creditors system - separation of duties / responsibilities	Separation between goods being received, invoices paid and authorised certification system						
			Budget monitoring	Budget monitoring by budget holders, management and Accountancy						
			Contract monitoring	Contract monitoring through contract register and authorisation etc.						
			Annual core system audit	This is a core system as decided by External Audit. This is audited annually by Internal Audit						
			National Fraud Initiative (NFI)	The Authority participates in the National Fraud Initiative e.g benefit claim matches are identified and investigated, cheques are security printed to comply with APACS standard. A copy also goes to Payroll.						
			Large cheques have to be signed individually	Large cheques have to be signed individually						
			Regular software checks done re valid list of suppliers.	Regular software checks done re valid list of suppliers.						
Fraudulent Bank Notes	Fraudulent Bank Notes	Loss of income to the Council	Scan Coin Machines have detection facilities in place	Scan coin machines have detection facilities in place	1	3	7	On Line Training - via SafeVoice	28/06/13	Dodd, Liz (Audit Manager)
			UV Marker pens in use	UV marker pens in use						
Fraudulent use of Corporate Credit Cards	Credit cards used for personal use	Misappropriation of funds. Criminal investigation. Reputation damage.	Training - on Corporate Credit Card system	Procedures for card holders and secretaries	1	2	4			
			Compliance with Credit Card procedures	Compliance with Credit Card procedures						

Risk Identified	Description	Potential Consequences	Control Measure	Description	Final Impact	Final Likelihood	Final Risk Rating	Further Action Required	Target Date	Owner		
Fraud Awareness											Risk Count:	34
			Review of policies	A review of control processes, in conjunction with management and HR								
			Monthly review of transactions and suppliers	Monthly review of transactions and suppliers by financial control, who review the nature of the transaction, and the types of supplier used.								
			Responsibilities formally allocated and agreed by cardholder	Credit card holders sign an agreement detailing their responsibilities								
			Credit Card - regular review of procedures by Internal Audit	As part of the Audit Plan, Internal Audit review the Credit Card policies, procedures and systems for effectiveness and compliance with statutory and professional guidance and best practice. Procedures updated: February 2013								
			Credit Card - separation of duties	Bills are paid by accounts payable. Procedures updated: February, 2013 - It is the responsibility of Authorised Users to complete the Credit Card Payment Authorisation (CCPA) form and to have it approved by the relevant Budget Holder and also by the Cardholder, in the spaces indicated. In the absence of the Cardholder, the form may be approved by an Authorised User, provided that the approver and the person who completed the form are not the same person.								
			£5,000 limit per month per corporate credit card	£5,000 limit per month per corporate credit card. Procedures updated February, 2013: The upper limit of a card will be determined by the Chief Executive in consulation with the Executive Director (Resources and Support Services) but may not be greater than £5,000 per month per card.								

Risk Identified	Description	Potential Consequences	Control Measure	Description	Final Impact	Final Likelihood	Final Risk Rating	Further Action Required	Target Date	Owner
Fraud Awareness										Risk Count: 34
Fraudulent use of investment money	Fraudulent use of investment money by Treasury Management staff	Insurance implications. Increase cost in insurance premium. Abuse in position. Abuse of public office. Financial implications. Reputation damage.	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 Carry out periodic reconciliations Separation of responsibilities for investments	Annual audit of treasury management Treasury Management meetings happen weekly Fidelity guarantee insurance for designated officers The Authority's policies, procedures and systems comply with and are based on statutory and professional guidance and best practice Use of Broker and Treasury Management advisors Carry out periodic reconciliations Separation of responsibilities for investments	2	1	2			
Fraudulently using external funding	Misuse or fraudulent use of external funding or fraudulent claim forms sent to external funding bodies	Reputation damage. Financial assistance would be cut off. Budgetary implications. Failure to deliver projects. Service delivery reduced.	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	Budget monitoring by budget holders, management and Accountancy Checks undertaken by external funding team and accountancy Newcastle Borough Council acts on lessons learnt Compliance with Financial Regulations Standing Orders in respect of contracts Independent verification of grant conditions Audit undertaken by internal and external audit & funding bodies if necessary	2	1	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	31/03/10 31/03/10 30/09/09	Sowerby, Simon (Business Improvement Manager) Sowerby, Simon (Business Improvement Manager) Roberts, Dave (Head of Finance)
Theft or misuse of the Authority's information	Theft or misuse of information, including personal data, credit card details and sensitive political information	Failure to work. Loss of Government Connects authorisation. Loss of data. Corruption of data. Financial gain. Reputational damage.	Clear desk policy Confidential information locked away Confidentiality clauses Encrypted memory sticks Access controls Saving data to servers Firewalls	Clear desk policy Confidential information locked away Confidentiality clauses Proper control of memory sticks Controls and passwords on systems Saving data to servers Firewalls	2	1	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	31/12/11 31/12/09 31/12/09 30/04/10	Baker, Dave (Head of Revenues & Benefits) Clisby, Paul (Head of Central Services) Hilton, Jeanette (Head of Customer & ICT Services) Whale, Cyd

Fraud Awareness

Risk Count: 34

Risk Identified	Description	Potential Consequences	Control Measure	Description	Final Impact	Final Likelihood	Final Risk Rating	Further Action Required	Target Date	Owner
			Information Security Policies	The Authority has a suite of 10 Information Security Policies based on professional guidance and best practice to ensure compliance with BS7799 or ISO equivalent.				Third party contracts in place for supply of OS data	31/12/09	Hilton, Jeanette (Head of Customer & ICT Services)
			Managing Information Risks risk assessment	Managing Information Risks risk assessment						
			Information Security Working Group	Information Security Working Group chaired by Esecutive Director - Resource & Support Services						
			Connected to Government Secure Intranet	Connected to Government Secure Intranet (gsi)						
			Inspire directive for sharing of data across EU	Inspire directive for sharing of data across EU						
			Metadata to ISO standards. Use of data for application.	Metadata to ISO standards. Use of data for application.						
Fraudulent use of council vehicles	Using Council vehicles for non council business	Breach of insurance cover. Criminal investigation. Reputation damage. Financial implications.	Vehicle logs	Vehicle logs maintained for each vehicle detailing journeys	2	1	2			
			Staff awareness of insurance implications	Staff awareness of insurance implications						
			Driving at work policy	Driving at work policy given to all employees with a driver risk assessment for them to complete						
Inappropriate receipts of gifts / hospitality	Officers receiving inappropriate gifts / hospitality	Officers open to bribery and corruption. Reputational damage.	Code of Conduct for Officers and Members	Email policy. Software blocking of certain words & sites.	1	1	1			
			Manager approval	Manager approval						
			Register of Interests	There is a central register for gifts and hospitality, and each Directorate keeps it's own register of outside interests and works for staff						
			Audit undertaken	Audit undertaken by internal and external audit & funding bodies if necessary						
			Staff informed of process	Staff made aware of what, when and how to record						
			Annual reminders	Annual reminders						
Theft or sale of official stocks / equipment	Theft or sale of official stocks / equipment for personal gain	Misappropriation of funds. Criminal investigation. Reputation damage. Loss of data. Corruption of data. Financial gain. Failure to work. Loss of Government Connects authorisation.	Regular independent checks of stocks / equipment across the council	Regular independent checks of stocks / equipment across the council	1	1	1	ICT to produce work programme to security mark all ICT equipment	31/12/09	Whale, Cyd

Risk Identified	Description	Potential Consequences	Control Measure	Description	Final Impact	Final Likelihood	Final Risk Rating	Further Action Required	Target Date	Owner
Fraud Awareness										Risk Count: 34
			Stock records maintained across all service areas within the council	Stock records maintained across all service areas across the council						
			Inventory of all ICT items (numbered)	Secure numbered nventory in place with periodic reviews						
			PCs are tagged/marked	PCs memory sticks, cameras are tagged/marked, security inbuilt in phones traceable through IP address.						
			Annual inventory checks	Annual inventory checks						
			Physical security	Equipment is secured in establishments and where necessary locked away. Ground floor offices have shutters on windows.						
Misappropriation of funds	Misappropriation of funds for services provided e.g. handyman, trade refuse, pest control	Abuse of position. Abuse of public office.	Minimising cash payments by debit card and direct payment methods	Minimising cash payments by debit card and direct payment methods	1	1	1	Documented clear work procedures to be produced	31/12/11	Heads of Service
			Regular independent reconciliations of funds	Regular independent reconciliations of funds						
			Cash secured	Cash secured						
			Cash and income collection - separation of duties	Cashing up and banking duties separated						
			Budget monitoring	Budget monitoring by budget holders, management and Accountancy						
			Whistleblowing policy	Whistleblowing policy						
			Financial Regulations	Compliance with Financial Regulations						
Fraudulent payments for personal gain	Payments made by BACS or CHAPS for personal gain	Misappropriation of funds. Criminal investigation. Reputation damage.	Independent reconciliations	Independent reconciliations	1	1	1			
			Approval process	Approval process						
			Budget monitoring	Budget monitoring by budget holders, management and Accountancy						
Fraudulent car loans	Employees claiming fraudulent car loans from the Authority.	Misappropriation of funds. Criminal investigation. Reputation damage.	Clear procedures for car loan applications	Clear procedures for car loan applications	1	1	1			
			Car Loans - separation of duties	Separation of responsibilities for approving car loans. Authorisation required by Chief Executive, Executive Director and Head of Central Services as part of the application process.						
			Affordability check	Direct payment of loan taken from salary each month						

Risk Identified	Description	Potential Consequences	Control Measure	Description	Final Impact	Final Likelihood	Final Risk Rating	Further Action Required	Target Date	Owner
Fraud Awareness										Risk Count: 34
Money laundering	Payments by proceeeds of crime	Criminal investigation. Reputation damage. Financial implications.	Money Laundering - statutory / professional guidance	The Authority's policies, procedures and systems comply with and are based on statutory and professional guidance and best practice	1	1	1	Money laundering training to be rolled out to staff	30/09/09	
			Audit review procedures and recommendations made	Audit review procedures and recommendations made						
			Cashiers audit	Review of payments of over £5000 in cash						
Agency staff claiming hours not worked	Agency staff submitting inaccurate timesheets or claiming hours they have not worked	Misappropriation of funds. Criminal investigation. Reputation damage.	Line manager checks hours worked	Line manager checks hours worked	1	1	1			
			Use of timekeeper system	Use of timekeeper system						
			HR involvement	HR involvement						
Theft from vulnerable people	Theft by staff from vulnerable people e.g. almshouses, welfare funeral homes	Misappropriation of funds. Criminal investigation. Reputation damage. Abuse of position. Abuse of public office.	CRB checks undertaken	Checks for all new staff and then every three years - cost £32 - £36.	1	1	1			
			Code of Conduct for Officers and Members	Email policy. Software blocking of certain words & sites.						
			Receipts given for valuables	Receipts given for valuables						
			Proper and safe handover procedures	Proper and safe handover procedures						
Theft of cash in transit	Theft of cash whilst being transferred from one establishment to another	Misappropriation of funds. Criminal investigation. Reputation damage.	Reducing cash transactions	Encourage people to pay by debit card or direct debit	1	1	1	Produce insurance risk assessment for process	30/09/09	Thornhill, Roger (Corporate Risk & Insurance Manager)
			Audit review procedures and recommendations made	Audit review procedures and recommendations made						
			Cash in transit - staff training	Cash in transit - staff training						
			Varying routes and drop off points, times etc	Varying routes and drop off points, times etc						
			Cybertrack phone issued to relevant staff	Cybertrack phone issued to relevant staff - there is an emergency button in case of attack etc						
			Handled by securicor / G4S	Handled by securicor / G4S						
Subletting of NBC properties	Letting of NBC properties for personal gain	Abuse of position. Abuse of public office. Criminal investigation.	Accurate details of premises to let	Accurate details of premises to let	1	1	1			
			Clear instructions to staff	Clear instructions to staff						
			Reconciliation of income	Reconciliation of income						
			Management checks of properties	Management checks of properties						

Risk Identified	Description	Potential Consequences	Control Measure	Description	Final Impact	Final Likelihood	Final Risk Rating	Further Action Required	Target Date	Owner
Fraud Awareness										Risk Count: 34
Abuse of telephones	Abuse of landline phones and mobile phones by staff	Misappropriation of funds. Criminal investigation. Reputation damage. Misappropriation of Council time.	Mobile phone provider	Monthly reports provided by Smith Bellaby	1	1	1	Regular reports to management to be produced	31/01/10	Whale, Cyd
			System in place for identifying personal calls and text messages	System in place for identifying personal calls and text messages						
			Telephone usage policy (corporate) in place	Telephone usage policy (corporate) in place						
			Register of Interests	There is a central register for gifts and hospitality, and each Directorate keeps it's own register of outside interests and works for staff						
			Regular telephone reports to management	Regular telephone reports to management						
Abuse of postage system	Abuse of postage and franking system by staff	Misappropriation of funds. Criminal investigation. Reputation damage.	Management check of postage costs	Monthly recharges done re postage costs to departments - would show on heads of service budget reports - any anomilies would show.	1	1	1			
			Budget monitoring	Budget monitoring by budget holders, management and Accountancy						
			Protocols set for handling of post	Protocols set for handling of post. Postal procedures updated: February, 2013.						
Abuse of internet	Staff using internet for personal use and viewing inappropriate sites	Misappropriation of Council time. Reputation damage.	Acceptable use policy signed by staff	Acceptable use policy signed by staff	1	1	1	Internet reports to be produced	31/05/10	Whale, Cyd
			Code of Conduct for Officers and Members	Email policy. Software blocking of certain words & sites.						
			Websense categories for certain web pages	Websense categories for certain web pages						
Payments to ghost employees	Payments to fictitious employees via payroll	Misappropriation of funds. Criminal investigation. Reputation damage.	Budget monitoring	Budget monitoring by budget holders, management and Accountancy	1	1	1	Implementing recommendations of HR audit - separation of duties	07/12/09	Durrant, Richard (Head of Human Resources)
			Payroll - Separation of duties	Separation and authorisation of setting new employees on the payroll						
			Review of payroll processes	These are reviewed as part of the restructure - creation of posts on establishment						
			Review of payroll system	The payroll system is subject to regular review and at times when there is a restructure within the Authority including establishment structure						
			Recruitment policy and process	Recruitment policy and process						

Fraud Awareness

Risk Count: 34

Risk Identified	Description	Potential Consequences	Control Measure	Description	Final Impact	Final Likelihood	Final Risk Rating	Further Action Required	Target Date	Owner
			Audit undertaken	Audit undertaken by internal and external audit & funding bodies if necessary						
			NFI checks completed annually	NFI checks completed annually						
Fraudulently trading for personal gain	Officers working for personal gain, including unauthorised work and private work. Abuse of position	Misappropriation of funds. Criminal investigation. Reputation damage. Abuse of position. Abuse of public office.	Code of Conduct for Officers and Members	Email policy. Software blocking of certain words & sites.	1	1	1			
			National Fraud Initiative (NFI)	The Authority participates in the National Fraud Initiative e.g benefit claim matches are identified and investigated, cheques are security printed to comply with APACS standard. A copy also goes to Payroll.						
			Register of Interests	There is a central register for gifts and hospitality, and each Directorate keeps it's own register of outside interests and works for staff						
			Checks by management	Checks done on email by Managers						
HR policies do not deter fraudulent behaviour	Not enough preventative controls or proactive action taken to deter fraud	Insurance implications. Financial implications. Criminal investigation. Reputation damage.	Review of policies	A review of control processes, in conjunction with management and HR	1	1	1			
			Disciplinary process	Disciplinary process to be followed, to act as a deterrent to others						
			Relevant stakeholders involved in review of processes	Relevant stakeholders including internal audit, are involved in review of processes						
			Anti-Fraud and Anti-Corruption Policy	Anti-Fraud and Anti-Corruption Policy						
			Whistleblowing policy	Whistleblowing policy						
			Managers Guide on Fraud	Managers Guide on Fraud						
			Related policies in place	Related policies in place - fraud & corruption, whistleblowing, corporate induction						
Fraudulent job application forms	Information contained in job application forms is fraudulent e.g. qualifications, job history, CRB checks	Inappropriate appointment. Security implications. Insurance implications. Financial implications. Criminal investigation. Reputation damage.	Obtain evidence of qualifications	Obtain evidence of qualifications	1	1	1	New policy linked to GCSX	30/09/10	Durrant, Richard (Head of Human Resources)
			Obtain references	Obtain references						
			HR involvement	HR involvement						
			Recruitment policy and process	Recruitment policy and process						
			Identity checks carried out	Identity checks carried out						

Risk Identified	Description	Potential Consequences	Control Measure	Description	Final Impact	Final Likelihood	Final Risk Rating	Further Action Required	Target Date	Owner
Fraud Awareness										Risk Count: 34
Fraudulent non attendance at work	Employees fraudulently not attending work e.g. fraudulent sick leave, extra holidays, flexitime, evening and weekend work, remote working	Abuse of contract. Abuse of public office. Abuse of position.	Checks of time by management	Checks of time by management	1	1	1			
			Reconciliation of leave	Management reconciliation of leave taken to leave cards and time recording system						
			Compliance with management of attendance policy for sickness	Compliance with management of attendance policy for sickness						
			Review of management of attendance policy	Review of management of attendance policy						
			Audit of management of attendance	Audit of management of attendance						
			Occupational Health to assist return to work	Occupational Health to assist return to work						
			Whistleblowing policy	Whistleblowing policy						