HEALTH & SAFETY EXECUTIVE FOR NORTHERN IRELAND

(HSENI)

FRAUD RISK PROFILE

August 2022

Definitions

Assessment of risk impact:

Low: Likely to impact on a small scale in the organisation if the risk occurs

Medium: Likely to have an impact on the organisation but not a serious one if the risk occurs

High: Likely to have a serious impact on the organisation if the risk occurs

Assessment of risk likelihood:

Low: Risk is unlikely to occur

Medium: It is possible that the risk may occur

High: It is very likely that the risk will occur

CASH HANDLING

How Fraud Could be Perpetrated	Initial Assessment of Impact of Inherent Risk	Initial Assessment of Likelihood of Inherent Risk	Examples of Controls	Residual Assessment of Impact of Inherent Risk	Residual Assessment of Likelihood of Inherent Risk	HSENI Business Area
Theft	Medium	Medium	• Hold cash securely at all times • Restrict access to cash to named personnel • Hold keys securely and limit access to authorised personnel • Keep cash balances to a minimum • Maintain transaction records • Petty cash ➢ All withdrawals of petty cash must be authorised by the budget holder and agreed to a receipt ➢ Carry out periodic checks and reconciliation ➢ Accounts Branch in DfE check reconciliations at year-end and at each request for petty cash top up	Low	Low	FMU
Income received not brought to account	Medium	Medium	• Issue pre-numbered receipts • Maintain prompt and accurate records of income received and ensure prompt lodgements. • Ensure post opening duties are carried out by at least two people and receipts log completed and signed by responsible officer • Separate duties at key stages in the process: ➢ Recording in valuables book	Low	Low	OST/ Comms/ FMU

How Fraud Could be Perpetrated	Initial Assessment of Impact of Inherent Risk	Initial Assessment of Likelihood of Inherent Risk	Examples of Controls	Residual Assessment of Impact of Inherent Risk	Residual Assessment of Likelihood of Inherent Risk	HSENI Business Area
			➢ Bringing receipts to account and preparation of cash and cheques for banking ➢ Invoicing and management of bad debts • Regular and random management checks of source documentation, accounting records and bank reconciliations.			
Illegal transfer or diversion of money. Changes and additions to payee details through BACS	Medium	Medium	**DRC Payments** • Changes can only be made via Account NI 'Supplier Maintenance' form • Form must be completed by two individuals, a preparer and an approver • Form must be approved and sent to Account NI by SO or above with accompanying email chain to prove that more than one individual has been involved in the process **Programme Payments** • Suppliers should only be added following the completion of a supplier form on the basis of information provided on a PR1 form signed by an appropriate budget holder • The supplier form must be signed off by a member of staff in FMU, SO or above	Medium	Low	All All

How Fraud Could be Perpetrated	Initial Assessment of Impact of Inherent Risk	Initial Assessment of Likelihood of Inherent Risk	Examples of Controls	Residual Assessment of Impact of Inherent Risk	Residual Assessment of Likelihood of Inherent Risk	HSENI Business Area
Accounting records are falsified or amended to allow unauthorised payments	Medium	Low	• Payments are only generated through the Creditors ledger, on invoice, so no journal entry will allow an unauthorised payment to be made • All payments must be approved by two signatories on online banking	Low	Low	FMU
Invoices are falsified or duplicated in order to generate false payment	Medium	Medium	**DRC Payments** In purchase order method of payment • Invoice must quote genuine purchase order number as generated via Account NI system payment • PO must be created and approved by two individuals, and the authoriser must be at a level of SO or above • Invoice is checked to ensure that it is mathematically correct • Invoice must quote unique invoice number • Goods received note (GRN) must be generated on the system before invoice can be paid • 3-way match of invoice, PO and GRN (within acceptable tolerance levels, otherwise invoice goes on hold) must take place before invoice is paid • In all other methods of payment, (Non-PO, AP 100) payment must be created and approved	Medium	Low	All

How Fraud Could be Perpetrated	Initial Assessment of Impact of Inherent Risk	Initial Assessment of Likelihood of Inherent Risk	Examples of Controls	Residual Assessment of Impact of Inherent Risk	Residual Assessment of Likelihood of Inherent Risk	HSENI Business Area
			by two individuals, and the authoriser must be at a level of SO or above **Programme Payments** • A PR1 form must be completed and signed off by an appropriately authorised budget holder as authorisation for work to be commissioned • PR1 includes requirement that Purchasing officer and Authorising Officer sign to declare they have no conflict of interest with the supplier • When invoice is received it is matched to the PR1 and sent to the appropriate budget holder for signature to authorise payment by email • Segregation of duties – FMU staff pay invoices but approval to pay comes from budget holders • Paid invoices are listed as paid in Content Manager • NAV system will not accept duplicate invoice numbers for the same supplier			All
Supplier bank account details are changed in order to divert payments	Medium	Medium	• Segregation of duties ➢ 2 officers within FMU or SMT approve payment on online banking on basis of signed invoice ➢ Invoice signed as approved by budget holder	Medium	Low	All

How Fraud Could be Perpetrated	Initial Assessment of Impact of Inherent Risk	Initial Assessment of Likelihood of Inherent Risk	Examples of Controls	Residual Assessment of Impact of Inherent Risk	Residual Assessment of Likelihood of Inherent Risk	HSENI Business Area
			➢ As per DAO (DFP) 08/13, suppliers are contacted independently to verify changes in bank details following requests in writing or by phone			
Unauthorised use of cheques	Medium	Low	• A very limited number of pre-printed cheques are kept in a locked cabinet in FMU and a few are held off-site in a locked safe in Netherleigh • Cheques have "a/c payee" printed across them • There are 8 signatories to the HSENI bank account; SMT and G7, DP and SO in FMU • Each cheque must be signed by two signatories, one of which must be a member of SMT.	Medium	Low	A small number of cheques are held in FMU and DfE for emergency use to make urgent payments if the BCP is invoked

PAYROLL/ TRAVEL AND SUBSISTENCE

How Fraud Could be Perpetrated	Initial Assessment of Impact of Inherent Risk	Initial Assessment of Likelihood of Inherent Risk	Examples of Controls	Residual Assessment of Impact of Inherent Risk	Residual Assessment of Likelihood of Inherent Risk	HSENI Business Area
Creating fictitious employees whose pay is then obtained by the fraudster or by someone in collusion, or obtaining pay that is not consistent with the employee's grade.	Medium	Low	• Ensure that only authorised personnel are able to inform HR Connect of updates to payroll records e.g leavers, starters, changes to existing data, temporary promotions. • Complete NFI Payroll exercises every 2 years (February 2021 completed – next one due February 2023) • Carry out monthly SOPCA report checks to ensure that each post is authorised, that the correct person is in post, that the person exists and that basic salaries and allowances are correct.	Medium	Low	FMU
Making false claims for allowances, travel and subsistence.	Medium	Low	• Abide by HR Connect Handbook Code (Section 9) & Account NI guidelines • Ensure checks by line managers of claims against approved work plans, work visits, meetings, standard mileage for destinations and primary evidence such as hotel bills, rail tickets, car parking tickets and taxi receipts are attached to claims • Checks completed by Corporate Support Group in relation to all Board members' travel and subsistence claims	Medium	Low	All

PURCHASING

How Fraud Could be Perpetrated	Initial Assessment of Impact of Inherent Risk	Initial Assessment of Likelihood of Inherent Risk	Examples of Controls	Residual Assessment of Impact of Inherent Risk	Residual Assessment of Likelihood of Inherent Risk	HSENI Business Area
Unauthorised use of purchasing systems in order to misappropriate goods or use services for personal gain.	Medium	Medium	• Restrict opportunity to generate payment by using sequentially numbered purchase orders • Establish authorised signatories and authorisation limits for requisitioning and placing orders and ensuring validity of purchase orders. • Match invoices with orders before the invoice is certified for payment. • Separate the duties between those ordering, receiving goods, and approving and paying invoices. This separation of duties should be reviewed regularly. • Ensure that authorised staff make amendments to standing data (e.g. supplier records). • Provide budget holders with sufficient and timely information to enable them to reconcile expenditure against budget. • Periodically review open purchase orders.	Medium	Low	All
Short deliveries of goods and services.	Medium	Low	• Check delivery notes to original orders, chase up short deliveries, and only pay for goods received.	Medium	Low	All

How Fraud Could be Perpetrated	Initial Assessment of Impact of Inherent Risk	Initial Assessment of Likelihood of Inherent Risk	Examples of Controls	Residual Assessment of Impact of Inherent Risk	Residual Assessment of Likelihood of Inherent Risk	HSENI Business Area
Acceptance of unsolicited goods or expanded orders as a result of attractions such as free gifts.	Medium	Low	• Confirm goods were properly ordered, authorised and received before authorising payment • Only pay for goods ordered	Medium	Low	All
Unauthorised booking of travel	Medium	Medium	• Maintain a list of authorised officers for booking travel (through the NICS contract) • Maintain a log of all transactions; that should be supported by authorisations to make purchases, invoices/receipts. (Authorisation should be at SMT level) • Check all entries on ACNI against invoices received and transactions logged • Reconcile transactions and balance on a monthly basis	Medium	Low	FMU

CONTRACTING

How Fraud Could be Perpetrated	Initial Assessment of Impact of Inherent Risk	Initial Assessment of Likelihood of Inherent Risk	Examples of Controls	Residual Assessment of Impact of Inherent Risk	Residual Assessment of Likelihood of Inherent Risk	HSENI Business Area
A contractor could be selected as a result of favouritism or who does not offer best value for money.	High	Medium	• Draw up and agree a clear and comprehensive specification • Seek tenders from suitable suppliers • Draw up clear and comprehensive tender evaluation criteria • Use of Central Procurement Directorate or a Centre of Procurement Expertise • Arrange for tenders to be delivered to those responsible for selection without interference • Do not accept late tenders • Ensure that tenders are evaluated against the agreed evaluation criteria by a tender evaluation board • Staff should have undergone CAL tender evaluation training where contract values are above EU thresholds • Staff should be required to declare any personal interests they may have which may affect the tendering process • Conduct appraisal prior to agreeing contract extensions in accordance with DoF guidelines, to include assessment of performance	Medium	Low	All

How Fraud Could be Perpetrated	Initial Assessment of Impact of Inherent Risk	Initial Assessment of Likelihood of Inherent Risk	Examples of Controls	Residual Assessment of Impact of Inherent Risk	Residual Assessment of Likelihood of Inherent Risk	HSENI Business Area
Payments made for work not carried out as a result of collusion between contractor and official	High	Medium	• Discuss forthcoming work when holding regular performance review meetings with contractors • Ensure that invoices are supported by independent certification that work was performed satisfactorily, and as agreed (e.g. through a media plan) before authorising payment • Maintain a register of contracts in progress • Only add approved and authorised contracts to the register • Ensure that all contract variations are adequately explained and appropriately authorised before payment • Invoices cannot be approved for payment by an addressee of the invoice	High	Low	All
A contractor could misrepresent third party costs and apply an unauthorised 'mark-up'	Medium	Medium	• Include the third party mark-up rate in the tender documentation • Obtain third party invoices when payment is sought and ensure that the tendered mark-up rate has been applied • Outline procurement requirements to the contractor and check these are being met (including spot-check of procurement documentation)	Low	Low	All

ASSETS

How Fraud Could be Perpetrated	Initial Assessment of Impact of Inherent Risk	Initial Assessment of Likelihood of Inherent Risk	Examples of Controls	Residual Assessment of Impact of Inherent Risk	Residual Assessment of Likelihood of Inherent Risk	HSENI Business Area
Theft or unauthorised use of assets	Medium	High	• Maintain up to date asset registers and inventories. (NAV Fixed Assets Register) • Clearly describe assets in registers and inventories • Mark assets in some way (e.g. property of HSENI). (Assets over £1,000) • Store assets securely • Carry out regular spot checks to confirm existence of assets. (Once per annum)	Medium	Low	Premises Officer/ FMU

INFORMATION

How Fraud Could be Perpetrated	Initial Assessment of Impact of Inherent Risk	Initial Assessment of Likelihood of Inherent Risk	Examples of Controls	Residual Assessment of Impact of Inherent Risk	Residual Assessment of Likelihood of Inherent Risk	HSENI Business Area
Theft or unauthorised access to sensitive/ restricted documentation, information or assets	High	Medium	• IT Assist filters internet access on behalf of Departments, primarily to limit access to websites that contain damaging or illegal content • Government Security Policy Framework • NICS Mobile Device Security Policy • NICS Use of Electronic Communications Policy • HSENI's Information Security Policy details the roles and responsibilities of HSENI staff (eg Senior Information Risk Owner, Information Asset Owners) and controls in place to manage information and cyber related risks • Define key roles and responsibilities for managing information risk (e.g. Senior Information Risk Owner, Information Asset Owners) and allocate to named individuals. • Establish an effective information risk governance framework. • Ensure that data security arrangements are underpinned by a culture that values and protects data. • Carry out regular assessments of the information risks and whenever changes occur to technology or new threats are identified • Restrict access to information on a "need to know basis"	High	Low	All

How Fraud Could be Perpetrated	Initial Assessment of Impact of Inherent Risk	Initial Assessment of Likelihood of Inherent Risk	Examples of Controls	Residual Assessment of Impact of Inherent Risk	Residual Assessment of Likelihood of Inherent Risk	HSENI Business Area
			• Ensure that access rights are reviewed regularly and that these are removed for staff that leave. • Limit the use of removable media (eg USB memory sticks). Encrypt data transferred to removable data • Devices with a data storage capability, for example, USB drives, external hard drives and CDs, which pose a significant security risk for the NICS, cannot be inserted on NICS PCs, laptops or personal devices • Ensure that all data users successfully undergo information risk awareness training. • Ensure that contingency arrangements (so that damaged or lost data can be renewed or replenished quickly) are regularly tested			

BRIBERY

How Fraud Could be Perpetrated	Initial Assessment of Impact of Inherent Risk	Initial Assessment of Likelihood of Inherent Risk	Examples of Controls	Residual Assessment of Impact of Inherent Risk	Residual Assessment of Likelihood of Inherent Risk	HSENI Business Area
Receiving a Bribe	Medium	Low	• Organisational culture of integrity promoted by senior staff. Also Standards of Conduct are set out in the HR Handbook – including Codes of Ethics and NI Core Values, Raising Concerns (Whistleblowing) procedures and guidance, Acceptance of Gifts, Hospitality and rewards guidance • Gifts and Hospitality Register on which staff are required to declare any gifts they have been offered, regardless of whether these have been declined or accepted • Raising Concerns (Whistleblowing) Guidance in place allowing both internal staff and external stakeholders to report suspected illegal activities, including fraud • Risk Register and processes in place	Medium	Low	All

CYBER FRAUD

How Fraud Could be Perpetrated	Initial Assessment of Impact of Inherent Risk	Initial Assessment of Likelihood of Inherent Risk	Examples of Controls	Residual Assessment of Impact of Inherent Risk	Residual Assessment of Likelihood of Inherent Risk	HSENI Business Area
Unauthorised or illegal access to HSENI network to gain access to bank details or other secure financial information which is used in a criminal manner	High	Medium	• Adherence to NICS Laptop and Information Mobile Device Security Policy and HSENI Information Security Policy • IT Assist Malware protection in place to prevent access from unauthorised or suspicious sources • All HSENI accounts are username and password protected • Annual Data Security Survey • Staff are required to complete the 'Cyber Security Awareness' e-learning programme	High	Low	All

GENERAL FRAUD

How Fraud Could be Perpetrated	Initial Assessment of Impact of Inherent Risk	Initial Assessment of Likelihood of Inherent Risk	Examples of Controls	Residual Assessment of Impact of Inherent Risk	Residual Assessment of Likelihood of Inherent Risk	HSENI Business Area
Internal fraud as a result of remote working, e.g. due to less direct supervision of staff	Medium	Medium	• Line managers having regular scheduled contact with team members • Reinforcement of culture/internal control messages e.g. through HSENI monthly newsletter (March 22 edition highlighted the release of NIAO Fraud Risk Guide and encouraged staff to familiarise themselves with it especially in the context of changing working arrangements brought about as a result of the Covid-19 pandemic)	Medium	Low	All

Reviewed by HSENI's Senior Management Team

Signed: Louis Burns

Date: 18 August 2022

Fraud Risk Profile - Document Information

Item	CM Reference
Document	HS2/22/16258
Container	HS1-13-189

Revision History

Issue	Date	Description of Changes
0.1	March 2013	Collation of existing Fraud Risk Profiles
0.2		Agreement by HSENI's SMT/ARMC
0.3	September 2015	Full document review to ensure fraud risks and controls are accurate and up to date and take account of recent DAO/FD guidance and changes in procedures.
0.4		Agreement by HSENI's SMT/ARMC
0.5	January 2016	Change made as a result of ARMC recommendation
0.6	March 2019	Document updated to reflect changes in systems/ roles since the document was last updated in January 2016.
0.7	August 2022	Document updated to reflect changes in systems/ roles, particularly in light of remote working practices implemented since the previous version.