# RISK PROFILE

## Financial - Fraud

Fraud in a healthcare organization can have significant negative impact on its finances, operations, employee morale, reputation, community/partner relations and credibility with funding agencies. This risk relates to theft and/or misappropriation of assets resulting from various means such as employee dishonesty, external scams (e.g. social engineering attack), cheque tampering, procurement fraud, benefits fraud, payroll fraud and vendor related scams. This document contains information entered by HIROC subscriber healthcare organizations (acute and non-acute) in the Risk Register application to help you in your assessment of this risk.

### Ranking/ratings[1]

- Likelihood – average score 2.29
- Impact – average score 2.88

**The Risk Register allows for risks to be assessed on a five-point likelihood and impact scale, with five being the highest.**

### Key controls/mitigation strategies

- Internal policies and processes
  - ✓ Formal Finance policies and processes such as Procurement policy, Employee Expense policy, Signing Authority policy
  - ✓ Other formal policies such as privacy, information security, gift acceptance, whistle blower, code of conduct and conflict of interest policies
  - ✓ Staff education and training on early identification and reporting of fraud
  - ✓ Social engineering training for Finance and Accounts Payable staff to identify fake e-mail, website and invoice scams
  - ✓ Segregation of duties (e.g. between cheque preparation and cheque signing, cash/cheque depositing and accounting data entry, cash management and statement/ledger reconciliation)
  - ✓ Signing authorities hierarchy including limits and second signature requirements
  - ✓ One level above approval requirement for expenses and cheque requisitions
  - ✓ Appropriate approval limits and processes for capital purchases
  - ✓ Documented request for proposal (RFP) evaluation and approval process
  - ✓ Proper background check on employees (e.g. vulnerable sector, criminal, credentials, reference)
  - ✓ Appropriate physical and technical safeguards implemented to monitor and restrict access to key financial information, signature stamps and cheques (e.g. camera, locked doors, safe, access controls to finance department folders, etc.)
  - ✓ Appropriate notification of terminated employees to Finance
  - ✓ Continuous communication between Finance and Human Resources departments to share information about fraud related activities
  - ✓ Strong relationship with banking staff to understand and adopt additional security measures
  - ✓ Appropriate network security controls and password policy
  - ✓ Close monitoring of outsourced finance activities (e.g. payroll, accounts payable)
  - ✓ Rotation of tasks within Finance

RISK REGISTER

# RISK PROFILE

## Financial - Fraud

- Vendor management
  - ✓ New vendor verification and set-up process (Check for credentials, physical address, telephone and website, names similar to employees or other vendors and references)
  - ✓ Approved vendor list is reviewed and updated regularly
  - ✓ Vendor invoices include itemized cost breakdown of services and/or products
  - ✓ Purchase order numbers are included in the invoice, where appropriate

- Protecting from cheque frauds
  - ✓ Electronic funds transfer (EFT) payments to staff, contractors and vendors (instead of cheque payments)
  - ✓ Adoption of various electronic safeguards to detect cheque tampering (e.g. Positive Pay Safe Check)

- Audits, assessments, checks and reconciliations
  - ✓ Adequate monitoring and controls in place ensure compliance with financial and other asset management policies
  - ✓ Daily/weekly/monthly/quarterly financial review and reconciliation process
  - ✓ Regular monitoring of invoices, payments and bank accounts for unusual activities
  - ✓ Regular review and reconciliation of payroll to identify fictitious employees
  - ✓ Internal audit function in place
  - ✓ Annual financial and internal controls audit, including audit of processes, by an external audit firm
  - ✓ Compliant with Payment Card Industry Data Security Standards (PCI DSS) if collecting, processing, transmitting or storing cardholder data
  - ✓ Fraud risk assessment is undertaken regularly to identify potential risk areas within the organization
  - ✓ Board level reporting of outcomes of internal and external reviews and audits

### Monitoring/indicators

- Fraud or theft related incidents and near misses
- Fraud detection capabilities and their effectiveness
- Employees, contractors and vendors set up on EFT
- Approved vendor list
- Potential fraudulent behaviours or indicators (e.g. drug or alcohol abuse, gambling, living beyond apparent means, reluctance to delegate work, limited or no vacation days off, preferred vendor contact)
- Comparisons of actuals to budgets
- Variance analysis
- Suspicious invoices, activities or accounts
- Internal signing authority hierarchy
- Annual financial and internal control audit results
- Bank audits
- Remediation plans based on the outliers identified during audits
- Compliance rates of finance related and information security controls
- Journal entry reviews
- Financial statement reviews
- Fraud audits from benefits provider
- Asset inventories (e.g. cheques, petty cash, major equipment)
- Unplanned procurement activities



RISK REGISTER

[1]As of January 1, 2018

Note: information presented in this document has been taken from the shared repository of risks captured by HIROC subscribers participating in the Integrated Risk Management program.