J Cassidy Business Focus Limited
https://www.jcbfl.co.uk
jane.cassidy@jcbfl.co.uk
+44 (0) 7717 705054 or +44 (0) 1920 872324
Registered in England & Wales - Reg. No. 11370541
Reg. Office: 69b The Maltings Business Centre, Roydon Road, Stanstead Abbotts, Hertfordshire SG12 8UU

[COMPANY NAME]

Risk & Control Matrix (RCM)

Control Function: [Board - Operational Risk - Fraud management]

Risk Ref / Sub Risk Ref	Risk Summary	Risk Description	Sub Risk Description
Board R1009 / Fraud Management R7001	Operational Risk	Lost profits, adverse publicity and reputational risk realisation, job loss and decreased morale and productivity through failure to detect, monitor and eradicate fraud risk	1. Financial loss through external fraud such as inflated or fraudulent claims. 2. Collusion either internally or with external third parties to facilitate fraudulent payments. 3. Underwriting outside authority to inflate contingent remuneration. 4. Submitting fraudulent expenses claims. 5. Recruiting dishonest staff or inappropriate (poor credit-worthiness) employees to financial positions. 6. Manipulating payroll to procure financial gain. 6. Employees procuring company assets for personal use.

RISK MANAGEMENT SELF-ASSESSMENT

RISK SCORING - before Controls			RISK SCORING - after Controls			
Risk Probability	Risk Impact	Total Score	Risk Probability	Risk Impact	Total Score = Residual Risk	Organisational Risk Tolerance/Risk Appetite
2	3	6	1	2	2	2. Within Risk Tolerance/Risk Appetite

CONTROL FRAMEWORK

CONTROL

Control Ref	Control Summary	Control activity	Control objective	Control owner	Control performer	Control frequency	Control type: Prevent, Detect	SOX 404 Control reference	Lloyd's Minimum Standard reference
Governance / Fraud O20001	Fraud policy	Up to date Policy which is subject to change control and approved by a sub-committee of the Board. The Policy is subject to regular monitoring by the Governance & Compliance Functions to ensure that the Policy provisions are understood and adhered to.	To mitigate the risk of a lack of fraud awareness and no tone at the top regarding Fraud prevention.	COO	Compliance Officer	Annual/ 3 monthly monitoring	Prevent / Detect	COSO	'MS4 – Governance, MS9 - Customer. MS10 Regulatory.
Governance / Fraud O20002	Board Risk Assessment	Board Risk Assessment	To aid in fraud detection and prevention in tune with the Board's risk appetite for alleviation of fraud and risk tolerance towards it.	Chair	Head of Compliance	Annual	Prevent	N/A - non financial controls	'MS4 – Governance, MS9 - Customer. MS10 Regulatory.
Governance / Fraud O20003	HR recruitment policies	Past employment verification, criminal background checks, credit checks, pre-employment medical screening, education verification, references checking.	To mitigate the risk of recruiting inappropriate new employees.	COO	Head of HR	Periodic	Prevent	N/A - non financial controls	'MS4 – Governance, MS9 - Customer. MS10 Regulatory.
Governance / Fraud O20004	HR remuneration & training policies	Anti-fraud training. Whistleblowing Policy which is embedded and monitored. Appropriate variable remuneration that is not a significant part of the overall remuneration package. Payroll controls.	To ensure that employees are disincentivised to commit fraud. Employees can report fraud anonymously and unencumbered. Employees are adequately trained in internal policies and procedures.	COO	Head of HR	Periodic	Prevent	N/A - non financial controls	'MS4 – Governance, MS9 - Customer. MS10 Regulatory.
Governance / Fraud O20005	Claims agreement and payment controls	Rigorous claims validation controls such as policy coverage checks, premium receipt. Payment validation controls.	To prevent the agreement and payment of fraudulent claims.	Head of Claims	Claims Director	Periodic	Prevent	COSO	'MS4 – Governance, MS9 - Customer. MS10 Regulatory.
Governance / Fraud O20006	Financial controls	Segregation of duties, use of authorisations matrix, dual sign-off, physical safeguards, job rotations, mandatory vacations. Validation of bank accounts independently for external third party payments (Invoices and claims).	To prevent financial loss through collusion and external fraudsters.	Financial Controller	CFO	Periodic	Prevent / Detect	COSO	'MS4 – Governance, MS9 - Customer. MS10 Regulatory.
Governance / Fraud O20007	Monitoring	Monitoring of Fraud through fraud reporting structure. Second line of defence monitoring of policies and procedures. Payment monitoring e.g. duplicate payments	To detect fraud and implement change where necessary.	COO / Compliance Committee	Compliance Officer	Periodic	Detect	COSO	'MS4 – Governance, MS9 - Customer. MS10 Regulatory.

INTERNAL AUDIT

INTERNAL AUDIT TESTING			INTERNAL AUDIT RATING		
Control Design audit test	Control Performance audit test	Audit Evidence	Control Design	Control Performance	Alignment with Self Assessment
Review and benchmark the Fraud Policies.	Assess for contemporaneous nature, effective change control and appropriate level of authority. Assess the effectiveness of the compliance monitoring of adherence to the Policy provisions.	Policy provisions. Review of committee papers to assess approval. Documentation of compliance monitoring activities.	Medium	Medium	YES
Review of the Board Risk Assessment for control design and control performance.	Ensure that the risk assessment is performed as prescribed.	Risk Assessment	Medium	Medium	YES
Review of recruitment policies for control design and control performance. Assess a sample of new starters for control effectiveness.	Assess a sample of new starters for control effectiveness.	Sample selection results.	Medium	Medium	YES
Review of remuneration policies for control design and performance.	Perform sample testing of training records and payroll set against employment contracts and bonus calculations.	Sample selection results.	Medium	Medium	YES
Review of claims agreement and payment controls	Claims sampling. Claims payments sampling.	Sample selection results.	Medium	Medium	YES
Review of Financial controls	Bank reconciliations. CAATs to evaluate large populations of payments. Review of authority matrix set against a sample of transactions.	Sample selection results.	Medium	Medium	YES
Review of the controls around the design of fraud reporting including timings, report direction.	Review of a sample of reports	Sample selection results.	Medium	Medium	YES