

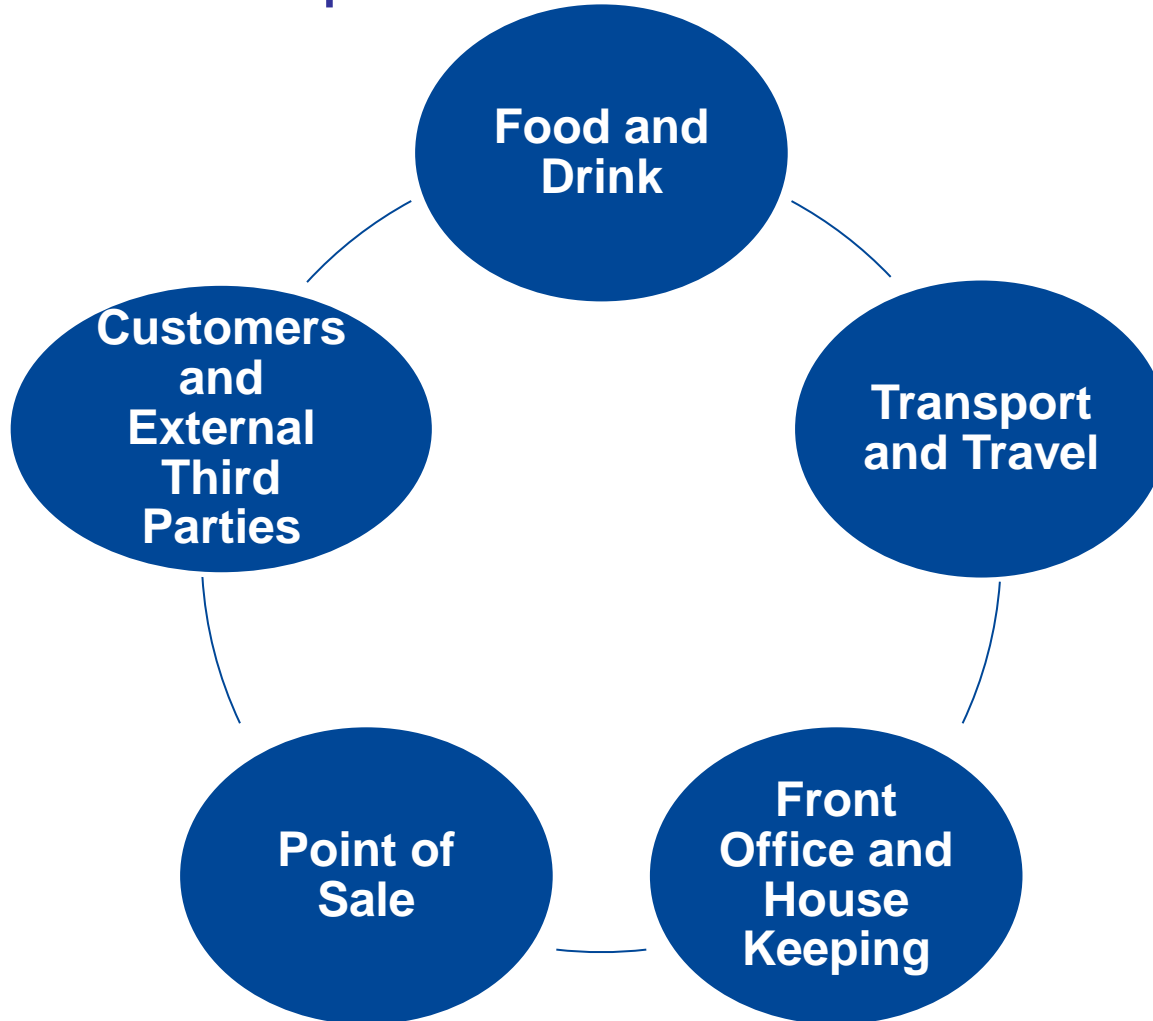


Fraud & Corruption Risks

John Baker

Risk Management Director, RSM Tenon

Operational Risk Areas





Operational Risk Areas

- Procurement/Purchasing/Payables
- Assets/Inventory
- Cash handling
- Money Laundering
- Staff, Payroll and Expenses
- Data theft



It could happen to you

- £4m restaurant fraud leaves ferry operator all at sea – staff fail to record sales and pocket the cash
- Seeing double after 250,000 counterfeit tickets sold – stolen blanks used to create duplicates of genuine copy
- Leisure centre manager's empire collapses – jail for finance manager who embezzled £42,000 from payroll
- No amnesty for hotel left to pick up the bill – 'cash back' scam used in name of a major international charity



You need to understand how and why fraud happens
in YOUR organisation

Error?

Opportunistic?

**Serial
fraudsters?**

**Organised and
networked
fraudsters?**



How do they get away with it?

- Complacency – are adequate controls in place to identify and monitor risk? Are the controls actually being used? And who checks these?
- Lack of Separation of Duties – trust is not a control
- Price to Pay – are appropriate actions taken to investigate and recover proceeds of crime?
- Learning Lessons - are you taking the right steps to mitigate risks and prevent them happening again?



Why should this matter to you?

1. Financial Loss –
 - funds or assets stolen
 - compensation to customers or business partners
 - fines
 - legal fees
2. Reputational Loss – potential loss of future business
3. Impact on Business Continuity – loss of experienced staff, time lost to deal with issues, potential for temporary inability to trade
4. Legal Implications – breaches of regulations or legislation such as the new UK Bribery Act



Ask yourself...

- Do you know the nature/scale of your fraud and corruption risks?
- How effective are your whistleblowing arrangements?
- What is the quality of the fraud awareness training provided to your staff?
- How do you prepare for fraud?
- Do you have a systematic means of learning from past fraud incidents, whether or not they occurred in your organisation?
- Do you understand how increased deployment of information technology (IT) assets can increase the risks of fraud?
- What is the effectiveness of your pre-employment screening systems?
- Is your counter-fraud strategy properly designed, up-to-date, and working...and how often are your key fraud-facing controls evaluated for relevance and effectiveness in a fast-changing environment?



The National Fraud Strategy – (good for the ‘demons’)

1. Create an anti-fraud culture
2. Deter fraud
3. Prevent fraud
4. Detect fraud
5. Investigate fraud
6. Apply appropriate sanctions
7. Redress the situation



Another way...good for the 80%

1. Create an ethical, fraud averse culture
2. Facilitate honest behaviour
3. Incentivise
4. Remind
5. Escalate
6. Investigate
7. Sanction
8. Redress the situation



Create an ethical, fraud averse culture

Facilitate honest behaviour

Use your data to target your efforts and resources

Deter, Prevent, Detect, Investigate, Sanction and Redress

Incentivise, Remind, Escalate, Investigate, Sanction and Redress

What about this?...could it capture the 90% (you don't have to worry about the 'angels')



What can you do about it?

- Fraud Risk Assessment – understand where your business is most at risk, what or who the risks are, and what you can do to reduce risks?
- Build robust and consistent systems and control processes to protect your business, maximise efficiency and establish an anti-fraud culture within the organisation
- Follow up all suspected fraud, corruption, theft or other abuse with an independent, professional investigation and where appropriate; disciplinary, civil, regulatory or criminal action



Do you have a handle on risk?

David Foley

Senior Risk Management Manager, RSM Tenon



Fraud Risks - insider enabled

- Recruitment fraud : immigration qualifications
non disclosure of previous criminal convictions, identity fraud
- Procurement
- Payment Systems
- Contractors: bogus / inflated invoices, work not conducted to specification
- Property / Assets – Use of
- Data Theft / Misuse
- Accounting Manipulation



Times when you may be most vulnerable to fraud

- Now
- Major personnel changes occur
- Departmental/organisational restructuring takes place
- New IT systems are brought in
- New policies/procedures are brought in
- Where there's a lack of audit coverage and/or supervision
- In times of recession...



Fraud Indicators

Behaviour

Results/
Performance

Documentation

Relationships
and other red
flags



Fraud Indicators - Behaviour

- Sudden change in lifestyle
- Extravagant spending
- Does not take holidays / refusal of promotion
- Unusually stressed
- Backlogs of work
- Lives beyond visible means
- Increase in number of hours worked
- First in, last out
- Controlling (particularly “experts”)



Fraud Indicators - Behaviour

- Suddenly antagonistic
- Obsessively bureaucratic (if out of character)
- Unwilling to improve controls
- Too co-operative
- Acts without approval
- Fails to delegate
- Reclusive/secretive



Fraud Indicators - Results

**Always meets
the budget**

**Unexpectedly
consistent
results**

**Always reports
early**

**High volume of
cash
transactions**

**Erratic
performance**

**Write-offs
outside normal
limits or high
volumes**



Fraud Indicators - Documentation

- Lost documentation
- Erased or crossed out figures
- Unusual *fonts* and inconsistent type faces
- High number of transactions of the same amount
- High levels of credit notes
- Poor tendering and selection processes
- Photocopies when originals would be expected
- Clearly falsified documents
- Documents re-written (on pretext of neatness)
- Lack of detail on documents



Relationships and other red flags

- Bullying individuals
- Unusual business structures/reporting lines
- Regular visits by same suppliers/excessive hospitality
- Unusual turnover of staff (high or low)
- Concerted efforts to avoid audit
- Unusual staff loans
- Unusual terms and conditions
- Claims outside normal levels



Fraud Indicators – Other red flags

- Unusual level of early terminations
- Patterns of awards and unusual and common price increases
- Disproportionate size of contract or geography
- Contracts that are not commercially viable
- Discrepancies in information
- Reconciliations that don't balance
- Unusual or unauthorised changes to systems and or procedures
- Large cash transactions
- Customer/Supplier/Staff matches



Best Practice

Basics:

- Segregation of duties
 - Budget Approval
 - Supplier and Goods/Services Selection and contract negotiation
 - Receipting
 - Approvals and Payments
- Standardised reporting systems
- Robust and workable policies
- Single (and approved suppliers) database, Contracts Register and payments addresses/bank accounts
- Strong Risk Management (don't simply rely on your Internal Auditors to identify issues)
- Robust Forecasting and Exception reporting



Best Practice

Basics:

- Detection Exercises (NFI, data analysis)
- Effective whistleblowing that staff are confident to use & is available to all who interact with you
- Know your risks and learn from others mistakes / bad experiences

Moving towards (if not already there):

- Implementing regular risk assessments to accurately identify your fraud risks
- A strong anti fraud culture (internally and with the people you do business with)
- Real (or as close as) time reporting
- Truly joined up systems
- Effective strategies to react effectively when fraud is identified



Questions to consider

Do you really know your fraud risks within your organisation?

- If so, are you assured your mechanisms are robust?

Is there a healthy anti fraud culture within your organisation?

Do we have a fraud response plan which all staff know about, which works?

Have we had any fraud occur?

- If not, is there none, are we picking it up, or should we proactively look?