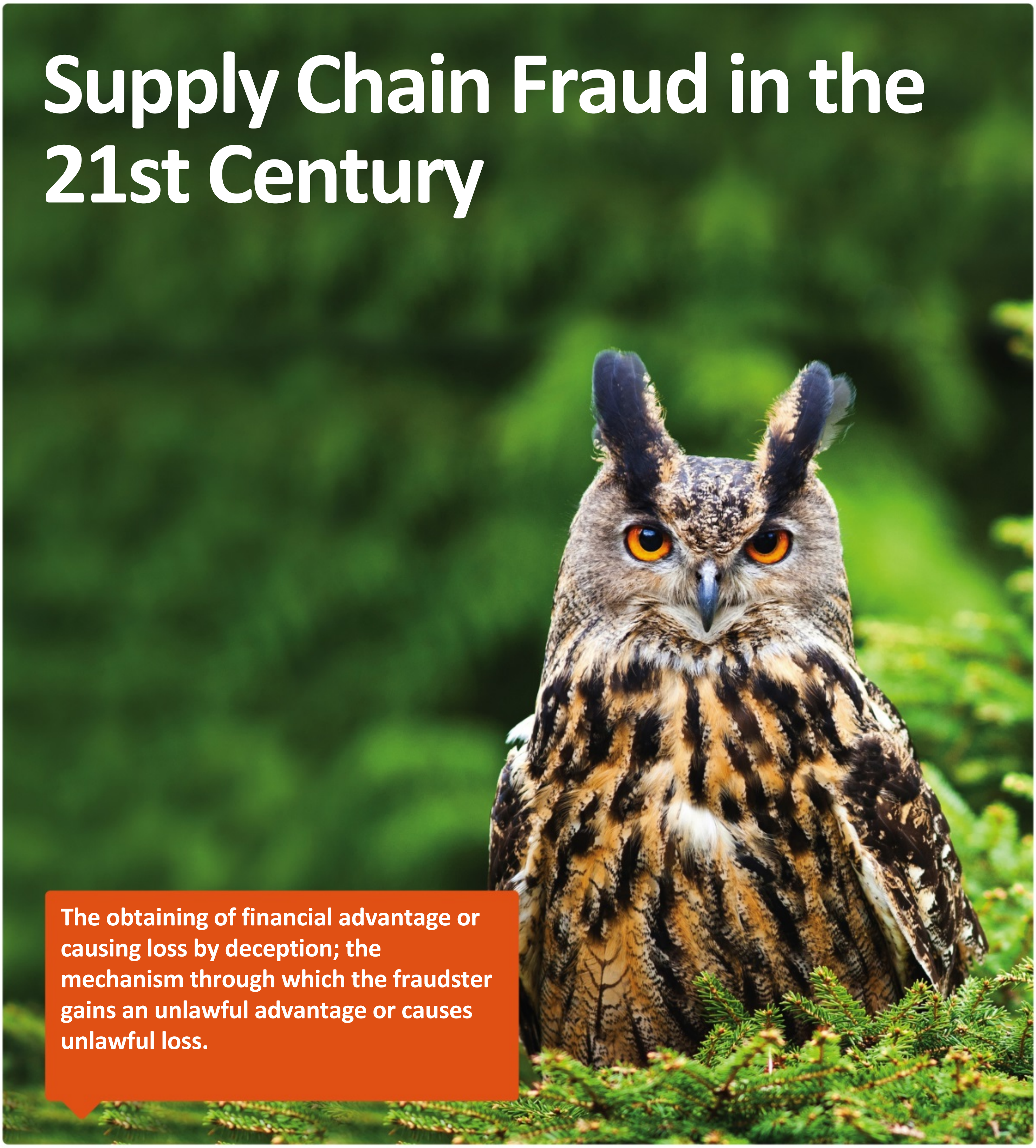
Knowledge Insight

CIPS KNOWLEDGE

Supply Chain Fraud in the 21st Century



The obtaining of financial advantage or causing loss by deception; the mechanism through which the fraudster gains an unlawful advantage or causes unlawful loss.

CIPS members can record one CPD hour for reading a CIPS Knowledge download that displays a CIPS CPD icon.

Leading global excellence in procurement and supply

Executive summary

Fraud is commonplace, wide-ranging, costly, and clearly affects the supply chain, as well as all other areas of corporate business. Fraud is also on the increase, especially with the development of IT systems and ever more sophisticated methods of perpetrating fraud.

Purchasing and Supply Management professionals have a duty to minimise the risk of fraud within the ambit of supply chain and supplier relationship management. There are many areas of the supply chain that might be affected by fraud and there are many different types of fraud. These are described in bullet-point form in this document. There is now one over-arching piece of legislation that covers all fraud. This is the Fraud Act 2006, which became law on 15 January 2007.

Scotland already had certain legal provisions to deal with fraud, so the act only applies in the rest of the United Kingdom. The new act replaces as many as eight statutory crimes and makes it much easier to prosecute fraud cases. Fraud is a risk, and should be formally managed as part of a corporate risk strategy.

Learning outcomes

The aims of this CIPS Knowledge Insight paper are to:

- learn definition of fraud
- learn to identify fraud and types of fraud
- learn about its impact on the global and local economy
- learn about the importance of eliminating fraud in the procure-to-pay arena
- learn that fraud is a criminal activity
- learn about the Fraud Act (2006), which tidies up confused legal position re: definition of fraud
- learn that there is empirical evidence that fraud is on the increase, especially Internet fraud
- learn about risk mitigation in fraud
- learn about policy for carrying out risk assessment for fraud.

Introduction and topic importance
The cost of fraud to the UK economy is believed to be in excess of £10 billion per annum. The cost to the world economy might be as high as between 3% and 6% of global GDP. The effect of fraud in financial terms is notoriously difficult to measure accurately. The impact of fraud is felt equally in both the public and private sector organisations.

Financial services markets are especially vulnerable. Plastic card fraud losses in 2005 alone were about £439m. The CIFAS (Credit Industry Fraud Avoidance System) database identified 85,128 fraud cases between January and June 2006, 12.5% up on the same period in 2005. The annual losses in the insurance market are estimated to be in excess of £550m. Fraud cost the telecoms market approximately £866m in 2004.

There are two separate victims of fraud: those who are ‘primary’ victims, who suffer directly from fraud, and those who are ‘secondary’ victims, who suffer vicariously. One major intangible ‘cost’ to victims is an emotional one, the effect on a person’s well-being as a result of their being defrauded. There is usually a greater relative impact on SMEs than on larger firms – although this is not always the case, take EXON, for example. Larger firms normally have the resources to recover from the effects of fraud. It is vital that all firms, but especially

SMEs, take steps to protect themselves against fraud or they could be rendered insolvent and their proprietors bankrupt.

Dealing with fraud should be part of an organisation's general corporate social responsibility (CSR) strategy. Organisations need to invest in proper supplier assurance programmes, including supplier accreditation to recognised pan-European standards.

There are many types of fraud. Some of the most prominent are as follows: counterfeit intellectual property, counterfeit money, data-compromise, embezzlement, insider dealing, market abuse, insurance fraud, fraudulent use of payment cards, procurement fraud, counterfeit products, consumer fraud, investment fraud, false accounting and reporting, bribery and corruption, collusion, false description, industrial espionage, theft, misappropriation of funds or assets, fraudulent administration of contracts, falsification of source records for fraudulent advantage, conflicts of interest, technological abuse.

Reduction in fraud is very important for supply chain managers. Little is reliably known about the extent and aggregate cost of fraud and there is a lack of reliable data for measurement. This lack of data complicates policy-making to deal with fraud.

The role of procurement in countering fraud

Purchasers have a duty to their employers to eradicate fraud. Procurement managers have a duty of care to their subordinates and also to their suppliers. Purchasers need adequate training to learn to identify fraud and subsequently to report on the risks flowing from types of fraud. It is important for them to realise that fraud costs organisations significant sums of money and lost profit.

It is also vital for supply-chain managers to include treatment of fraud as part of risk and business continuity planning. Firms should adopt as a minimum benchmark CIPS' Code of Ethics. Corporate disciplinary procedures should provide that transgressors of the CIPS code can be dismissed, as well as 'struck off' by the Institute itself. It is important for organisations to establish what is acceptable or unacceptable hospitality.

There should be a clear policy on what are and are not unsolicited gifts. It is imperative that policies are put in place that lead to the eradication of favouritism towards, and cosy relationships with, suppliers. Checks and balances should be implemented to mitigate against any misuse of p-cards. These controls should also aim to remove, inter alia, the following:

- payment for work not carried out
- duplicate payments and the creation of false suppliers in ERP solutions
- payment for short deliveries and so on
- suppliers carrying out personal work for corporate employees
- cases of personal benefit from corporate supply contracts where there is no policy to allow for such benefits.

Definitions

For the purpose of this Knowledge Works paper we will define fraud as: 'The obtaining of financial advantage or causing loss by deception; the mechanism through which the fraudster gains an unlawful advantage or causes unlawful loss.'

The most common types are frauds are defined below:

Corruption – meaning the payment or receipt of any unauthorised benefit to or by an agent (usually an employee) for doing, or not doing, anything in relation to his work. Examples include:

- acceptance by an employee of cash for influencing a decision made on behalf of his employer
- payment of club membership for an employee of a supplier in return for favourable treatment
- indefensibly lavish entertaining of, or by, an employee with the possible intention of influencing a decision.

Conflicts of interest – where agents (again usually employees) have private, undisclosed interests that could interfere with their work and fiduciary obligations to their principles. Examples Include:

- engaging in part-time work or consultancy, without permission
- using sensitive company information for personal benefit, including insider dealing
- drug or alcohol abuse, which affect work performance.

Theft of assets – including the unauthorised removal of intellectual capital and information. Examples include:

- theft, embezzlement, false accounting, and deception
- theft or misuse of proprietary information
- malingering and theft of time paid for by the company
- commercial deception by suppliers, customers, and others.

False reporting and falsifying performance – this includes both the creation of false reports and suppression of material information. Examples include:

- submitting false accounts to conceal inadequate performance or to qualify for a bonus
- using false accounts to deceive investors, bankers, a stock exchange or a third party
- manipulating financial results
- suppression of regulatory and other breaches and false reporting; examples include: falsely reporting compliance with environmental, anti-discriminatory or other regulatory requirements; fraudulently concealing violations of money laundering, health and safety, human rights or other regulations.

Technological abuse – including unauthorised access to computer systems, implanting viruses or other malicious code, and sabotage. Examples include:

- accessing computer files without authority
- unauthorised Internet browsing
- computer related fraud.

CIPS views, opinions and beliefs are stated throughout the document. However, the broad practice statements that underpin the text are as follows:

CIPS position on practice

CIPS firmly believes that Purchasing and Supply Management professionals should;

- be trained to have an understanding of fraud and the likely circumstances in which fraud might occur in their organisations
- maintain a suitable body of knowledge about fraud cases and the types of fraud that can occur in their markets, at home and abroad

- have a full understanding of rules, regulations, laws and guidelines relating to UK and global fraud
- ensure that checks for fraud form part of all vendor assessment and supplier evaluation programmes
- formalise commercial anti-fraud policy within the main procurement strategy document
- strive to minimise bottom-line financial loss to their organisation arising from fraud
- review, analyse and challenge all supply-chain business processes to mitigate the possibility of fraud in each one.

Relevant legislation

The Fraud Act 2006

The Fraud Act 2006 came into effect on 15th January 2007 and applies to England, Wales and Northern Ireland. Apart from Section 10 (1) relating to Section 458 of the Companies Act 1985, it does not apply to Scotland. This Act largely replaces the laws relating to obtaining property by deception, obtaining a pecuniary advantage and other offences created under the Theft Act 1978. These offences attracted much criticism for their undue complexity and difficulty of proving guilt in court.

The Fraud Act establishes a new general offence of fraud which can be committed in three ways:

- Fraud by false representation - Section 2: this is committed if a person makes “any representation as to fact or law... which is express or implied” and which that person knows to be untrue.
- Fraud by failing to disclose information - Section 3: this is defined as where a person fails to disclose any information to a third party when that person is under a legal duty to disclose such information.
- Fraud by abuse of position - Section 4: this occurs where a person occupies a position in which he or she is expected to safeguard the financial interests of another person, but abuses that position. This includes cases where the abuse consists of an omission, as well as an overt act.

In all three classes of fraud, for an offence to have occurred, the person must have acted dishonestly, and with the intent of making a gain for themselves or anyone else, or inflicting a loss (or a risk of a loss) on another. ‘Representation’ must be as to fact or law, including a representation as to the state of mind of the person making the representation or any other person. This can be express or implied.

A ‘gain’ or a ‘loss’ is defined as consisting of a gain or a loss only in money or other property (including intangible property) but could be temporary or permanent. A ‘gain’ can be construed as gaining by keeping existing possessions, not just by obtaining new ones. A ‘loss’ can include losses of expected acquisitions, as well as losses of already held property.

The Act also establishes two ‘supporting’ offences, one being the possession of articles for use in frauds (Section 7); the other being the making or supplying of articles for use in frauds (Section 8). For example, under Section 8, writing software knowing that it is designed or adapted for use in connection with fraud can result in a custodial sentence of up to 10 years.
Section 12 of the Act provides that where an offence against the Act is committed by a body corporate, but is carried out with the ‘consent or connivance’ of any director, manager, secretary or officer of the company, or any person purporting to be such, then that person, as well as the body corporate, is liable. An important difference between this Act and the Theft

Act 1978 is that offences against the Fraud Act do not require there to have been a victim, as was the case with the Theft Act. Conviction carries a maximum sentence of 10 years and/or an unlimited fine.

The Competition Act 1998

The Competition Act 1998 came into force on the 1st March 2000 and introduces two main prohibitions:

1. A prohibition of anti-competitive agreements, which are intended to, or have the effect of, 'preventing, restricting or distorting competition in the UK'. The Act also covers situations where there is no actual agreement, but where the actions of trade associations or companies acting together have the same effect.
2. A prohibition of abuse of a dominant position in the UK or part of the UK. Such actions include 'limiting production, markets or technical development to the detriment of the consumer'. The intention of this Act is to create a regulatory framework that is tough on those who seek to impair competition, but allows those who do compete fairly the opportunity to thrive. Key aspects of this legislation are:

- anti-competitive agreements, cartels and abuses of a dominant position are unlawful from the outset
- businesses which infringe these prohibitions are liable to financial penalties of up to 10% of UK turnover for up to 3 years
- competitors and customers are entitled to seek damages
- the Director General of Fair Trading has powers to step in at the outset to stop anti-competitive behaviour
- investigators are able to launch "dawn raids" and to enter premises using reasonable force
- a leniency policy will make it easier for cartels to be exposed.

Computer Misuse Act 1990

The Computer Misuse Act became law in August 1990. It is designed to meet the general threat of unauthorised access, often called 'hacking', and the introduction of viruses. There are three offences in the Act:

1. Unauthorised access to computer material (such as a program or data): A person is guilty of an offence if he or she causes a computer to perform any function with intent to secure access to any program or data held in a computer AND access or intended access is unauthorised AND that person knows this is the case when the action is carried out. Unauthorised access to computer material is the lowest level of offence and includes such practices as finding or guessing someone's password and/or using another's password to access a computer system.

   The offence occurs even if no changes to data are made and no damage is done. It is the act of accessing materials without authorisation that is illegal. It carries a penalty of up to six months imprisonment and/or a maximum fine of £2,000.

2. Unauthorised access to a computer system with intent to commit or facilitate committing further offences: This expands on the first offence and includes gaining access to financial or administrative records.

   It is the term 'intent to commit or facilitate committing further offences' that increases both the severity of the offence and the severity of the possible penalty, which is up to five years' imprisonment and/or a fine.

3. Unauthorised modification to computer material: This offence includes such practices as deleting files, changing the desktop build, introducing both local and networked viruses and modifying system files.

   The key element of this offence is "intent" that is, it is aimed at deliberate acts. It extends to the access of one computer through which damage is perpetrated on another remote computer. This offence carries a penalty of up to five years imprisonment and/or a fine.

NB: CIPS legal commentaries do not purport to be any more than a brief summary of the law. There are many other areas of law which have an impact in this area, including laws on insider dealing and money laundering under UK and EU law on which specialist advice should be sought. If the reader is in any doubt then independent, expert legal advice must be sought.

Impact of fraud

The impact of fraud on an organisation is far reaching. On a corporate level the following issues apply:

- impacts on bottom line, cost, asset valuation and utilisation, corporate asset acquisition and disposal
- impacts on customer/client/stakeholder records and support
- relates to all aspects of business and commerce
- effects shareholder confidence and share values
- brings loss of operational integrity
- adds to litigation and insurance costs
- impacts on staff morale
- reduces credibility of management
- diverts management resources
- subverts organisation's strategic objectives and policies
- impairs brand value/image and lessens the balance-sheet value of goodwill
- increases reputational risk
- impacts on corporate standards
- must be seen in the wider context of managing all risks
- must identify the processes or activities at risk of fraud
- risk to product and service outputs/deliverables
- risk to operational areas/locations
- risk to revenue generation/profitability
- risk to cash flow
- risk of unbudgeted increases in expenditure.

There are also many issues that impact P&SM professionals directly. P&SM professionals should consider the following issues and their relation to the purchasing department, policies, processes and procedures:

- strongly contiguous to corruption
- has a place in CSR strategy
- is fundamental in buyer-supplier relationships
- weak P2P processes and systems allow it
- risk to supplies and inputs.

Areas of weakness

We have all heard the saying 'prevention is better than cure' in the case of corporate fraud nothing rings more true. cSo what can P&SM professionals do to ensure that any measures implemented reduce the likelihood that their organisation will be victimised by any P&SM related fraud? The following list details potential areas of weakness encouraging fraud which require monitoring and addressing:

- poor anti-fraud and corruption strategies
- weak risk management strategies.
- slack controls on people, suppliers and business processes
- anti-whistleblowing culture and lack of protection for whistleblowers
- poor accountability and governance
- poor scrutiny
- weak checks and balances, internal and external monitoring and auditing
- inadequate staff training on fraud
- making it more difficult to spot fraud
- little notable punishment for transgression
- inadequately documented policy and procedure for fraud
- failure to identify fraud indicators, such as stress levels, refusal to take leave, unexplained wealth, cosy relationships with suppliers
- lack of encouragement of prevention
- lack of positive promotion of detection
- lack of clear pathways for fraud investigation
- failure to change culture and behaviour of people
- laissez-faire attitude and approach to fraud
- lack of openness in organisation
- poor staff training on fraud
- fraud is easily perpetrated
- inadequate formal, documented policy and procedure for fraud
- lack of understanding in organisations of corporate fraud response practices.
- lack of clearly defined business processes
- willingness to encourage bribery to match international culture and expectations in buying and selling abroad
- unsatisfactory processes, poor division of roles and responsibilities
- encouraging perpetration of fraud.

Measures to take to implement policies

It is important that all P&SM personnel should be trained so that they have a detailed understanding of the risks in the operation under their own span of control; and a broader overview of wider business risks. One way of achieving this is by a process in which P&SM professionals review the risks and controls, and agree between themselves the measures for improvement. Secondly, P&SM professionals should maintain a body of knowledge that informs them of the type of frauds that can occur in the markets and countries in which they acquire goods and services.

Due to the many rules, guidelines, laws and regulations both nationally and internationally on organisational compliance, there is a greater onus to ensure that P&SM professionals are aware of their responsibilities. Not understanding these compliance obligations is no excuse.

This is an area within business that cannot be left to chance, as it is easy to make mistakes, and if concealed, can have very serious consequences. In fact, fraud and concealment or failure to comply with laws, rules and regulations can be regarded as equal risks.

The following outlines the measures P&SM professionals should consider when implementing policies:

- ensure a formal declaration of vested interests programme is established
- create a policy for the declaration of gifts and hospitality and methods of dealing with these
- ensure that a strong segregation of duties policy is established and formalised
- ensure that confidentiality and nondisclosure policies are not too narrow and secretive and, where appropriate, observe the requirements of freedom of information legislation
- ensure that formal non-collusion statements are signed at the relevant stage in any tendering process
- link codes of conduct to the disciplinary process and contracts of employment, use CIPS code of ethics as the minimum standard, be prepared to dismiss staff found guilty of fraudulent practices, be prepared to bring in the police
- create the necessary checks and balances by implementing internal audit or external forensic audit controls and processes
- ensure 'gateway' reviews are carried out at each stage of a procurement project; the focus of reviews is to 'investigate and challenge'
- consider installing two separate 'whistleblowers' hot-lines', one for staff, one for suppliers, and investigate all complaints received from any source
- regularly review standing lists of suppliers
- ensure that tender evaluation criteria for contract award are objective, fair and non-discriminatory; consider separating quality and price tenders and not allowing any through to the price stage unless they have passed the quality threshold
- incorporate strong security measures (lock down computers and increase firewalls) into corporate ICT policy
- ensure that the policy is well known and understood by employees and other stakeholders
- carry out regular training and awareness sessions for employees.

Frequently asked questions

Where can I find information on other legislation regarding fraud?

- Transparency International – 'Transparency International, the global civil society organisation leading the fight against corruption, brings people together in a powerful worldwide coalition to end the devastating impact of corruption on men, women and children around the world.'
- CIFAS is the UK's Fraud Prevention Service with 260 members spread across banking, credit card companies, asset finance, retail credit, mail order, insurance, savings and investments, telecommunications, factoring, and share dealing
- EUROPA is the portal site of the European Union. It provides up-to-date coverage of European Union affairs and essential information on European integration. Users can also consult all legislation currently in force or under discussion, access the websites of each of the EU institutions and find out about the policies administered by the European Union under the powers devolved to it by the Treaties
- CIPS legal helpline is free to all CIPS members – 0800 0921980.

What steps can I take to minimise the risk of fraud inside the procurement and supply chain functions of my organisation?

- develop a suite of guidance material and formal business processes that act as enablers for those involved in procurement in the organisation
- conduct a full risk analysis in P&SM and highlight key areas of vulnerability
- identify which preventative measures exist elsewhere in one's organisation and consider their application in procurement and supply chain management
- ensure that anti-fraud measures and their application are driven from the very top of the organisation
- develop a robust P&SM fraud policy that reflects the commitments formalised by senior management
- implement a risk management strategy in P&SM and create a risk register with actions necessary to mitigate key risks
- ensure that the penalty for fraud committed by employees is rigidly enforced.

I am often told that fraud 'directly effects the bottom line'. What are the other ways in which fraud can damage our business?

- fraud lowers staff morale and creates mistrust
- fraud creates adverse publicity for the organisation
- fraud causes significant damage to the organisation in the eyes of its suppliers, customers and shareholders/stakeholders
- the organisation suffers severe disruption from a major fraud investigation
- fraud can lead to bankruptcy, firms being put into administration (especially SME's) and jail for owners/employees.

Staff motivation and discipline are particularly sensitive issues in my organisation. What steps can I take to reduce the risk of fraud without seeming to be swinging the heavy jackboot at staff?

- employees are to be at the heart of any anti-fraud strategy. The rule is: 'velvet glove, iron fist.' Reward loyalty and do not discriminate on grounds of age, sex and so on
- discreetly check and confirm all references
- define each employee's responsibilities clearly and make sure they know who they should report to if problems arise
- avoid having 'indispensable' staff who alone know the workings of a particular part of the business
- many frauds require regular activity by the fraudster. Make sure everyone takes regular breaks from work Remember - the bigger and more sophisticated the fraud, the more likely it will be that senior staff are involved
- ensure sensible staff rotation policies are implemented, where it is appropriate to do so
- ensure that relationships between suppliers and buyers are never close and personal
- ensure that you have an holistic corporate procurement strategy that effectively deals with procurement in 'satellite' parts of the organisation
- ensure that you have satisfactory risk assessment, surveillance and audit processes that can lead to the identification of fraud at an early stage
- keep up-to-date on emerging fraud threats
- Ensure that ordering, receiving and paying responsibilities are segregated.

I need to beef up the way managers deal with fraud in my organisation. I know I need to lay on extra training for them, but what should I do about the organisation's management controls? I think they're weak, too.

- review all of your management control systems (including any embedded in IT systems) and identify any weaknesses. Take advice from specialists if you are uncertain

- always check bank and trade references of suppliers and clients through trade protection organisations or credit reference agencies
- protect your financial position by asking new clients for part payment in advance or make only partial deliveries. You can also ask for personal guarantees - credit insurance is another option
- if you are suspicious of an individual, remember that details of bankrupts are held at your local Official Receivers' office. Details of disqualified directors are kept by Companies House, and are available on the Internet free of charge at: Companies House website
- have a clear company policy relating to fraud, and stick to it. Review it regularly. Ensure a senior manager or director has overall responsibility for fraud management
- come down hard on irregularities
- set an example from the top
- inform and train staff
- inform suppliers of your policy
- encourage "whistle-blowing" but be prepared to protect any member of staff who does so
- use the advice of internal auditors or non-executive directors
- remember, dissatisfied employees are more likely to be tempted by fraud
- if necessary access police records and security services checks
- ensure that duties and responsibilities which encourage fraud are segregated appropriately
- vet, train and monitor temporary agency and interim management staff, including external consultants and advisors
- use CCTV to conduct surveillance in high-risk areas
- introduce spot checks on activities, stock and personnel as appropriate.

My organisation is becoming ever more dependent upon computers to manage the back-office processes which underpin the services we deliver. How can I improve computer security so that fraudulent ICT practices are minimised?

- have a clear policy concerning the use of computer systems
- change passwords regularly and keep them confidential
- consider sourcing an externally-hosted service, or outsourcing parts or all of the ICT service, rather than keeping it all in-house. External providers should have far greater skills and controls in minimising fraud
- ensure all staff are aware of their legal standing with regards to their use of computers
- employ staff who are suitably trained in the use of the IT systems
- take regular and frequent backups of data and keep copies of backups off the premises in case of theft, fire or other disaster
- install anti-virus software and firewalls to prevent fraudulent practices and lock down pc's to prevent employee access to inappropriate websites (online gambling and so on)
- beware of computer viruses through unsolicited discs or through the Internet
- implement and maintain a corporate disaster recovery strategy and test plans regularly and frequently
- seek the advice of experts if unsure.

Further Reading

- Comer, Michael J., InvestigatingCorporate Fraud, price: £59.95, ISBN: 0566085313, pages: 245.
- Sadgrove, Kit, The Complete Guide to Business Risk Management, 2nd ed., price £65.00, ISBN 0566086611, pages: 348.

- Ed., Reuvid, Jonathan, Managing Business Risk - A Practical Guide to Protecting Your Business, 3rd Ed., Price: £50.00 , ISBN: 0749445106 , pages: 317.

Useful Websites

.transparency.org/
.homeoffice.gov.uk/
.cifas.org.uk/
.apacs.org.uk/
.acpo.police.uk/

Author

Ron Hardwick
Chairman
Contracts SKG
Friday, 17 August 2007

CIPS would like to thank the Contract Specialist knowledge group for their contribution to this paper.

CIPS
KNOWLEDGE

CIPS Group Easton House, Easton on the Hill, Stamford, Lincolnshire, PE9 3NZ, United Kingdom
T +44 (0)1780 756777 F +44 (0)1780 751610 E info@cips.org

CIPS Africa Ground Floor, Building B, 48 Sovereign Drive, Route 21 Corporate Park, Irene X30, Centurion, Pretoria, South Africa
T +27 (0)12 345 6177 F +27 (0)12 345 3309 E infosa@cips.org.za

CIPS Australasia Level 8, 520 Collins Street, Melbourne, Victoria 3000, Australia
T 1300 765 142/+61 (0)3 9629 6000 F 1300 765 143/+61 (0)3 9620 5488 E info@cipsa.com.au

CIPS Middle East & North Africa Office 1703, The Fairmont Hotel, Sheikh Zayed Road, PO Box 49042, Dubai, United Arab Emirates
T +971 (0)4 327 7348 F +971 (0)4 332 5541 E mena.enquiries@cips.org