A strong defence

MARTIN O'DONOVAN LOOKS AT THE CONTROLS AGAINST FRAUD THAT SHOULD BE PUT IN PLACE.

Executive summary

Fraud is an ever-present danger for every company. All organisations need to ensure that they have the policies and procedures in place to minimise their risk of falling victim to fraud. This article discusses what can go wrong, the main controls to prevent fraud and the current regulatory and legal framework.

The massive losses incurred at Société Generálé remind us that we are all vulnerable but we can and must do a great deal to prevent such events. Embedding good anti-fraud controls is not difficult but it does require a commitment to take seriously what can appear minor steps and procedures. However, taken together these minor steps will add up to a strong defence. The best deterrent for fraud is creating a control environment and company culture where the chance of detection is high.

Unless a fraud is particularly large or in some way scandalous it tends not to hit the news, but fraud is still widespread and a very real risk. Deflecting cash, paper or electronic payments is an obvious danger but fraud also takes in the theft of goods, inflating personal expenses, infringement of intellectual property rights such as using software without the proper licence, and could involve accounting manipulation. This latter case may mean the inflation of sales figures to generate increased personal bonuses, or just for the sake of personal pride and maintaining a reputation, or making some adjustments to cover up other mistakes. In the world of treasury dealing there may be no motive for personal gain – a dealer may run up unauthorised positions in the belief that his speculation will boost company profits.

WHAT CAN GO WRONG In a treasury and cash management function the most obvious danger is that payments are made to unauthorised third party accounts. Blank cheques could be stolen, or valid cheques intercepted and fraudulently altered. Physical controls and care over cheque writing should be straightforward – avoiding such carelessness as cheques payable to B T which can easily be changed to another name like B Tomlinson. Banks should be able to advise on security features and styles of printing to prevent alterations. Paper-based payments are vulnerable to misuse through interception in your own organisation, in the postal system and at their destination and in any case are expensive to process. There is a current trend away from paper-based payments towards e-payments driven by cost savings, efficiency and the desire for straight-through processing (STP), but in addition going electronic has the added benefit of reducing many of the opportunities for fraud.

False invoices could be introduced into the accounts payable section, or valid invoices used to deflect payments to the wrong accounts. It is important that efforts are directed at checking goods received against invoices and orders and having the right internal sign offs. However, in addition companies should not forget about the controls over standing data – namely the suppliers' bank account details. Falsifying a request from a supplier supposedly providing new bank account details is not difficult, so controls to check the validity of the change request are essential.

Treasury originated payments as a matter of routine can be very large indeed so even just one error or fraud could be disastrous. Companies may direct unusual or one-off payments via the treasury department so the utmost caution is needed. Standard Settlement Instructions (SSI) limit the chances of wrong payments and as with supplier details extra strong controls are required over changes to SSIs. At least with electronic payment instructions controls and multiple levels of authorisation can be built in but who authorises the authorisers?

In a notable UK treasury fraud £9m went astray over time to meet a gambling habit. New authorisers had been set up but these new members of staff had never been told and the fraudster kept all the identities for himself.

Most forms of control rely on division of responsibilities so

that no one individual can undertake a transaction or approval on his own. Yet on every dealing desk the dealer can routinely bind the company instantly over the phone or at the press of a key. Unauthorised position taking is naturally a weak spot and here some of the crucial controls come after the event. So speed is of the essence to ensure controls like reporting and position monitoring and matching of confirmations are performed.

PREVENTION Starting from the top, a good governance structure and clear policies will set the framework and corporate culture, which is then translated into practical working procedures. These will define the sequences of actions required to perform the daily tasks, what information is required and how it flows with the firm, what is recorded and reported and monitored.

Limits will be set to establish authority limits as to what may be done or approved by each individual and in the case of treasury dealing there will be counterparty and position limits.

This leads into segregation of duties (see Box 1) which lies at the core of all controls. If there is wholesale collusion in the section where the fraud is originated and in the functions charged with monitoring, then you are done for. A rigorous internal audit function can counter this as will a well publicised arrangement for whistle-blowing. But if the concept of introducing multiple checks and sign offs is to work, the authoriser at the end of the chain has not only to check that the underlying transaction is valid and reasonable but importantly their job is to check that the prior approvals have been properly made and recorded. When the final authoriser signs off an invoice for payment he may be required to check that the approval form has been signed off as goods properly received and matched to order, but does that authoriser really recognise all the signatures of those back along the approval chain? A systems-based process is far more reliable with controls built in to require a certain pattern of sign-offs by the appropriate people. In this case a robust IT administration is required. The administrator should be independent of the operators and not have a sole level of access that would in itself pose a risk, such as amending the core control features.

Automation has its strengths but when a company is designing an automated system it is important to consider the documentation and audit trail and think about the stage at which the organisation is most vulnerable. If invoice payments are fully automated not only is the control of payment account details important but you may find that the logging of the order onto the system becomes the critical point from which everything else flows, so are you absolutely sure the order is valid in the first place? For treasury dealing documentation takes the shape of exchange and matching of confirmations, now ideally electronic, and is a key control along with the escalation procedures for mismatches.

The procedures for confirmations will be covered in the dealing mandate a company has with its bank as will the procedures for notifying SSI. An organisation will also want to lay down the names of the legal counterparties that are covered, the instruments covered and the authority limits for individuals, but on these details some banks are becoming more and more reluctant to accept limitations. The advice is to negotiate hard, after all presumably they want the business, and ultimately a company must decide if it is prepared to deal with a bank that does not take this element of control seriously. Stressing the theme of "who authorises the authorisers" your mandate will need to cover the process for changes to the mandate.

Management reporting is a further layer of control. This can be risk based to concentrate on the important data, and be designed to be timely, clear, concise and focused using exception reporting, benchmarks and Key Performance Indicators (KPIs) as appropriate. Too much or too muddled reporting may itself turn into a weak spot.

DANGER SIGNALS Let us not forget the human side of fraud, and the proper screening of candidates at the recruitment stage. Then look out for:

- The employee who fails to take his annual leave allowance.
- The employee who regularly is at his desk early and works long hours and is reluctant to delegate or share responsibilities.
- Unusual changes in lifestyle – the new upmarket car.
- Some personal crisis at home.
- A passion for gambling or addiction to other expensive habits.

In the notorious 1994 Orange County case of inappropriate instruments and speculation, the county treasurer, Robert Citron, was reported as rarely taking a vacation and staff found him prickly, secretive, controlling and arrogant. The dealer John Rusnak in Allied Irish Banks' Allfirst subsidiary lost $691m in 2002 and enjoyed entertainment, wining and

Box 1: Segregation of duties

Segregation of duties is designed to prevent fraud and detect errors. It is particularly important where large sums of money are transferred and to detect breaches of counter party limits or positions.

The general principle is to break up the transaction into several steps and make several people responsible for implementing it. Typical steps are:

- authorisation: the initial approval.
- execution: doing the transaction.
- custody: delivering, receiving.
- recording: entering the transaction into the recording system.
- checking: independently verifying the copy of the third party's record of the transaction, with that of the company.

In a small treasury, limited staff numbers may make segregation of duties difficult. In this situation, some functions may have to be performed outside the treasury, and in any case this can provide added independence.

dining and the back office found him arrogant and abusive. That is not to say it represents conclusive evidence!

DETECTION Implementing the layers of controls should be worth while in the first place but they need not be regarded as a cost burden. Good controls and anti-fraud measures should mesh in with good business and management processes. Management reporting and monitoring that helps decision making can serve a dual purpose. Indeed the Sarbanes-Oxley Act (SOX) applicable to companies with a US listing demands an adequate internal control set up.

Taking matters a stage further, proactive fraud detection measures can be built in to systems and reporting e.g. a targeted data filtering tool or intelligent system to identify anomalous activity. Risk reviews and assessments can direct internal audit to vulnerable areas. Take any tip offs seriously and be alert to warning signals. Many frauds are detected through external tip offs or just by accident.

THE FRAUD ACT The Fraud Act 2006 came into force on 15 January 2007. It clarified the criminal law in the UK since until then there was no criminal offence of "fraud". The Act creates a new general offence of fraud which can be committed in three different ways:

- by false representation.
- by failing to disclose information.
- by abuse of position.

Thus it is an offence dishonestly to abuse one's position, where one person is in a privileged position and expected not to act against another's financial interests. This position exists, for example, between director and company, professional person and client, and certainly between employee and employer.

RECOVERY AND INSURANCE Good controls will materially reduce the chances of loss from fraud, but nonetheless it is still normal for companies to take out fidelity insurance. This sort of insurance gives cover for losses incurred as a result of fraudulent or dishonest acts by employees or specified individuals. A condition of the policy will be to have certain core controls in place and working.

Should a fraud be detected it is necessary to move swiftly. Calling in the police may be the first reaction but many companies in the end prefer to rely on civil proceedings if it is thought there is a good chance of securing some recovery or redress. The civil process allows businesses to retain some control and would get held up until after any criminal proceedings have been dealt with. The courts are willing to grant a variety of search orders, freezing orders and disclosure orders, although if recoveries are being sought from abroad the procedures are inevitably more complicated. Speed is important if the missing assets are to be found before they have been disposed of, so having a contingency plan in place and suitable legal contacts available would be prudent.

In your eagerness to be seen to be reacting the temptation might be to sack the suspected fraudster, but it would be safer to suspend him and remove him from the premises so as to be able to secure any evidence. IT evidence on a server or personal computer could include incriminating evidence, but care is needed in reviewing files so as not to interfere with any records and access logs that prove the suspect had access.

There is also the question of publicity and minimising any adverse PR or even dealing with business interruption or financial consequences like breaches of covenants. All of which calls for some pre-thinking and an internal plan to deal with any major fraud event.

Effective anti-fraud policies and working procedures require a degree of rigour and commitment from the company and its management.

This level of financial management and control is a central tenet of a well run operation and required as part of compliance with regulation and guidance such as SOX and Turnbull. The central theme is that there is no excuse for ignoring the potential for fraud.

INTERNAL CONTROL STANDARDS General advice on internal controls across an entire business has been issued by the US-based Committee of Sponsoring Organizations of the Treadway Commission (COSO). Founded in 1985 it is now a voluntary private sector organisation focused on improving the quality of financial reporting through business ethics, effective internal controls and corporate governance. COSO identifies five key components of internal control: 1) control environment, 2) risk assessment, 3) control activities, 4) information and communication, and 5) monitoring.

Martin O'Donovan, ACT's Assistant Director – Policy and Technical.
modonovan@treasurers.org
www.treasurers.org