

Facing up to fraud.

The need for a risk-based approach



Fraud Risk Management

Times are changing fast. In October 2004 the Financial Services Authority ('FSA') unveiled its new regulatory approach to dealing with financial fraud. The FSA has now put financial fraud risk management on its agenda of 'risk-based' regulation through its existing supervisory regime it will seek to measure and evaluate the degree of compliance with expected best practice. Notwithstanding this announcement, the FSA also published a report in November 2004 highlighting concerns over poor IT security which may be exploited to commit financial fraud through internal or external attacks on firms' IT infrastructure.

Equally publications such as ISA 240 and the Basel Committee on Banking Supervision's paper number 96 on Operational Risk have underlined the critical nature of internal and external fraud risks and the need for institutions to have appropriate fraud risk management systems in place with appropriate management responsibility and oversight to manage these vulnerabilities.

It will therefore be increasingly important for management teams to operate in the knowledge that they have reviewed their fraud risk management strategies and methodologies to ensure that they are appropriate and will withstand regulatory scrutiny. Management will need to demonstrate a serious commitment to dealing with financial fraud risk and be able to talk in an informed fashion about their relevant systems and controls within the context of a 'risk-based' approach.

Any institution subject to the requirements of Sarbanes-Oxley will already need to be addressing such issues whether as a US listed company or as a 'foreign-based issuer'.

Reducing the risk of fraud is an achievable corporate objective

Effective fraud risk management and the design and implementation of effective preventative and detective strategies requires a joined-up understanding of the risks associated with a firm's operational cornerstones – people, process, and technology and a willingness on the part of all stakeholders to face up to the difficult questions of "could it, and might it happen to us – and how?" It also requires adopting measures that transform corporate culture, establish an effective control environment, and secure data assets.

Assessing vulnerabilities

An important first step in limiting an organisation's potential exposure to financial fraud risk is to conduct a targeted assessment of where its vulnerabilities lay, both from an internal and external perspective. Such an assessment drives the question of how people might, if intent on doing so, extract value from the organisation, at any level of seniority, acting alone or in collusion. It will also involve looking at the risk of money laundering and at the security of its IT infrastructure which underpins the entirety of its business operations.

Facing up to fraud

Deloitte methodology

We are frequently called on by our clients to help them when they suspect they may be victims of fraud or are worried that they are about to become so. We do not sell a standard 'product' because there is no such thing as a standard client. All our clients' concerns are unique so we do not follow the 'one size fits all' approach. Instead we have developed a proven suite of methodologies that can provide an integrated approach to fraud risk management which is scaleable and relevant to your needs. Our individually tailored services are designed and executed by fraud experts and IT security specialists who have real industry experience in the prevention, detection and investigation of financial fraud.

The Deloitte fraud risk management methodology can include any or all of the following features to assist you in fraud prevention, detection and investigation by providing cost-effective recommendations and action plans to enable you to effectively manage your fraud risks. In addition to the services listed below, we can also offer tailored fraud risk management training courses.

Vulnerability Diagnostic

A top down review of your fraud and information security policies, procedures and strategies together with an organisation's fraud risk management framework, which, combined with interviews and discussions with selected staff, seeks to identify potential legal and regulatory compliance issues such as FSA, Sarbanes-Oxley and COSO requirements providing high-level feedback on your operational approach.

D&Termine

A web-enabled survey tool that provides a valuable insight into your organisation's ethical culture and actual impact of fraud programs from staff and management. Using D&Termine, specific yet anonymous feedback is sought that will enable you to understand employee perceptions of the key factors that may be either contributing to or mitigating fraud vulnerabilities. It also provides detailed analysis of employee understanding and awareness of issues relating to fraud.

Vulnerability Workshops

Highly participative, and conducted with a cross section of staff and management, workshops enable the identification and prioritisation of specific financial fraud vulnerabilities. For prioritised and agreed vulnerabilities across your people, process or technology we can review existing controls, systems and procedures and identify potential fraud risks.

D&Tect

A powerful suite of data analysis tools designed to identify potential fraud and control weaknesses by data mining the information held within the business. It can be used on a standalone basis utilising fraud profiles developed on the basis of past investigations or used to drill down into the higher risk areas identified in the workshops or through D&Termine.

Information Security

Our information security specialists are aware of security vulnerabilities that IT systems are exposed to and can translate these technical issues into 'jargon' free business terms.

Our information security specialists are aware of business as well as technical issues and understand the need to see information security issues in terms of business risk and are able to explain complex technical problems in 'jargon' free business terms.

We use an established methodology, proprietary techniques and tools, and the results of our own ongoing research, to perform advanced comprehensive tests of your applications or network to identify any computer systems vulnerable to internal or external attack.

Our IT security specialists can work with your staff to assist in the implementation of both remedial and new sustainable security initiatives.



All IT systems have some degree of vulnerability; the important thing is to know where to focus your efforts in order to get best return on your security investment. We have methodologies to assist you in improving the effectiveness and efficiency of your vulnerability management and risk remediation processes. Using the existing tools within your organisation we can help you prioritise system vulnerabilities according to your threat profile.

Fraud investigation

Whether investigating a large scale international fraud requiring the tracing of cross-border transactions, employee malfeasance, procurement fraud, corruption or general accounting irregularities, our Financial Fraud Investigations team has extensive experience in dealing with the increasingly prevalent and complex problem of white collar crime.

We tailor our approach to each case, selecting from proven methodologies, leading software and electronic investigative tools. At each stage, we have the skills and experience to help you: gathering, securing and preserving the evidence; interviewing suspects, employees and witnesses; recovering assets; assistance in presenting the case in court or at a disciplinary hearing; and finally provision of recommendations for improving your systems and controls to reduce the risk of a similar incident happening again.

Forensic Technology

If you were hacked would you know what to do? Would you know how far the breach had gone? Could you contain the problem? How would you clean up and how are you going to prevent it from happening again?

In the event of fraud occurring, we are one of the few organisations who have the necessary skills and evidential data recovery resources to respond effectively. We can recover digital evidence to Police, Serious Fraud Office, FBI and UK and US court standards from a variety of IT equipment.

Subsequent data analysis is necessary to investigate and present evidence in a clear and concise format we can use our IT forensics expertise to analyse large volumes of electronic information effectively to quantify the fraud and support any litigation process.

We can also investigate how fraudsters have gained access to your systems so that you can close any 'open doors' that have been left open.

Experienced, Qualified Practitioners

Our consultants include forensic accountants, lawyers, former law enforcement officers, IT forensics technologists and information security specialists. Their credentials are second to none in terms of industry experience and recognised certifications, qualifications and accreditations from some of the industry's most respected bodies. In addition, many of our consultants are CLAS and CHECK registered and UK Government security cleared. Through the use of balanced teams we can deliver a truly multi-disciplinary approach to any situation.

For more information, please contact:

Nic Carrington
Partner, Forensic and Dispute Services
Tel: +44 (0) 20 7303 2139
Email: ncarrington@deloitte.co.uk

Simon X. Owen
Partner, Information Security
Tel: +44 (0) 20 7303 7219
Email: sxowen@deloitte.co.uk



For further information, visit our website at www.deloitte.co.uk

In this publication references to Deloitte are references to Deloitte & Touche LLP. Deloitte & Touche LLP is a member firm of Deloitte Touche Tohmatsu.

Deloitte Touche Tohmatsu is a Swiss Verein (association), and, as such, neither Deloitte Touche Tohmatsu nor any of its member firms has any liability for each other's acts or omissions. Each member firm is a separate and independent legal entity operating under the names "Deloitte", "Deloitte Touche Tohmatsu", or other, related names. The services described herein are provided by the member firms and not by the Deloitte Touche Tohmatsu Verein.

Deloitte & Touche LLP is authorised and regulated by the Financial Services Authority.

This publication has been written in general terms and therefore cannot be relied on to cover specific situations; application of the principles set out will depend upon the particular circumstances involved and we recommend that you obtain professional advice before acting or refraining from acting on any of the contents of this publication.

Deloitte & Touche LLP would be pleased to advise readers on how to apply the principles set out in this publication to their specific circumstances. Deloitte & Touche LLP accepts no duty of care or liability for any loss occasioned to any person acting or refraining from action as a result of any material in this publication.

© Deloitte & Touche LLP 2004. All rights reserved.

Deloitte & Touche LLP is a limited liability partnership registered in England and Wales with registered number OC303675. A list of members' names is available for inspection at Stonecutter Court, 1 Stonecutter Street, London EC4A 4TR, United Kingdom, the firm's principal place of business and registered office.
Tel: +44 (0) 20 7936 3000. Fax: +44 (0) 20 7583 1198.

Designed and produced by The Creative Studio at Deloitte, London.

Member of
Deloitte Touche Tohmatsu