

risky businesses

Grant Thornton periodical
reporting on risk and improvement
services for business owners.

Grant Thornton 

Financial fraud, an unpleasant reality

Do you have effective controls to protect your business?

A new study shows that corporate fraud is flourishing in Australia and New Zealand, fuelled by lax internal control frameworks and a lack of awareness. In the US in particular, internal control frameworks have grown in importance in recent years, with improvements driven by the US Sarbanes-Oxley Act, which places great importance on internal control systems.

Financial fraud and corporate collapse

Speaking on the subject of material financial fraud, ASIC Chairman Mr. Jeffery Lucy addressed the risk of material internal financial fraud.

According to Mr Lucy, ASIC's experience highlights material financial fraud as one of the key factors in corporate collapse. He flagged prevention as one of the major future challenges we face.

Looking at the most recent, significant, and highly publicised corporate collapses in Australia and overseas, Mr Lucy pointed out that the overwhelming majority involved material financial fraud. Companies that collapsed from commercial causes (eg Ansett) are in the minority. However, collapses such as WorldCom, Enron, Adelphia, Parmalat and, in Australia, HIH, Clifford Corporation, Harris Scarfe and possibly Sons of Gwalia, each involved systematic fraudulent actions.

Clearly, strong internal controls and probity of an independent audit committee are necessary measures to safeguard against financial fraud. These may be achieved by putting in place effective corporate governance structures and arming its audit committee with a charter to test, detect and root-out fraud.

How small businesses react

Drawing on data from the Small Business Crime Survey, we find a significant variation in reporting crimes to the police. Influencing factors included the type of crime and whether the crime was attempted or completed.

The survey's statistics on incidents that were reported to police are:

- nine out of ten completed reports relating to burglaries and robberies
- only one in 17 incidents of employee theft
- one in five incidents of shoplifting
- one in four incidents of cheque/credit card fraud.

Reasons for non-reporting varied, but most commonly reflected a pessimistic belief that reporting crime was pointless and achieved nothing.

Businesses appear to be largely unaware of the threat of fraud. While the study indicated that fraud was a major problem for business generally, the losses are not regarded as significant by the businesses.

It's time businesses woke up! Without effective fraud control, organisations are making themselves prime targets for fraudsters. It's important to note a disturbing trend: the perpetrator typically comes from within the organisation, has no known history of dishonesty and is usually a long serving employee.

How internal control provides management assurance

Effective internal controls help safeguard an organisation's assets, prevent irregularity and fraud, promote operational efficiency and encourage adherence to management policies.

Internal control is an integral part of an organisation's management. Its aim is to provide reasonable assurance that the organisation's objectives are being met in the following categories:

- effectiveness and efficiency
- reliability of financial reporting
- compliance with laws and regulations
- safeguarding and accountability of assets (including company's funds and cash)
- preventing and detecting errors and fraud
- achieving targets through effective stewardship of company's resources.

Effective internal controls should achieve the following general objectives:

- orderly, ethical, economical, efficient and effective operations
- fulfilling accountability obligations, whereby management and those charged with governance as well as the individuals within the organisation are held responsible for their decisions and actions. These include stewardship and all aspects of performance
- compliance with laws and regulations
- safeguarding resources against loss, misuse, and damage due to waste, abuse, mismanagement, errors, fraud and irregularities.

Making it work...without overkill

In the post-Enron era, there has been criticism that there is overkill in the application of internal controls and corporate governance, spawning a corporate culture of risk avoidance. CFOs, directors and auditors are saying that they have had a gutful of the changes the new regulations have imposed on them and they want to focus on making improvements to their existing systems. They are expressing concerns about the cost of internal controls required by Boards and management to ensure the level of control they have over their companies' systems and processes.

There is a convincing argument that effective internal controls enable management to extract value from the systems and processes they have spent so much time and money embedding in order to deliver valuable information to management, their investors and auditors. Managers and regulators need to accept that the effectiveness of an internal control regime is only as good as the culture in which it is embedded.

The central proposition is that implementing a system to prevent fraud is one thing, creating a climate in which people don't wish to commit it is another.

It is therefore the responsibility of management and those charged with governance to:

- integrate cost-effective internal control into all of its operations
- monitor the effectiveness of its internal control operations and the outcomes.

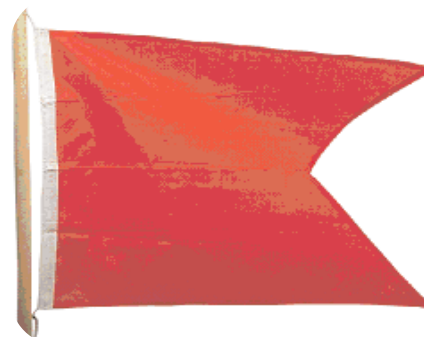
Get back to basics

- improve your culture - understand that fraud is linked with culture and does not depend wholly on internal controls
- automate your controls
- maintain your risk framework
- institute an internal control programme
- ask 'what can go wrong' questions
- conduct a fraud 'health check' - identify red flags.

Ask these questions

- Has your organisation undergone major change such as new responsibilities, reorganisation, funding cuts, expansion of programs, or changes in management?
- Are you understaffed and/or has workload drastically increased?
- Are your staff having difficulties handling operational workload?
- Do your employees understand which behaviour is acceptable or unacceptable?
- Are your employees satisfied or generally disgruntled?
- Is top management aware of actions taken at the lower level of the organisation?
- Is there lack of clarity around roles, responsibilities and accountability?
- Is the organisational structure inefficient or dysfunctional?

Depending on the answers, you may need to address the red flags. We have to recognise that fraud is a real threat. Your business is not immune, but there are ways to protect it. Remember, the way your organisation functions can have a major effect on the incidence of fraud.



How safe is your Virtual Private Network?

What is VPN?

A Virtual Private Network (VPN) is a private communications network usually used within a company, or by several different companies or organisations, to communicate over a public network.

How does VPN work?

A VPN uses public telecommunications infrastructure like the internet, to allow remote access to corporate resources. Instead of using a dedicated connection, such as a leased line, VPNs use connections routed through the internet from the company's private network to the remote site. The remote site can be an employee working from home or other location, such as a hotel, library, cyber café, or seminar conference room.

Remote access security is a major issue

As the use of VPNs continues to increase in the workplace, remote access security has become a major issue facing IT departments. Today, many organisations pay more attention to ensuring the integrity of data flowing between remote access clients or end users and corporate networks. Unfortunately, less focus is placed on endpoint security, which is a highly critical area.

Endpoint security is the branch of IT security that is concerned with controlling the threats to remote computers. While most VPN tunnels - secure network-to-network connections across the public internet - are relatively immune to snooping and data modification, remote computers running VPN clients are susceptible to attacks. This is why remote computers remain one of the most vulnerable IT asset exposing organisations to security breaches.

There is a critical need to audit VPNs. Due to the distributed nature of threats, it can be particularly difficult for IT departments and internal auditors to identify and monitor VPN security risks. Many IT departments are loaded with other security-related tasks and don't have time to make sure remote computers are not vulnerable to attacks.

To ensure VPN channels are secure, internal auditors must work with IT departments to identify endpoint security threats and make sure detected vulnerabilities are patched immediately and properly.

Virus Threats

Virus threats and spyware are some of the most common threats to VPN. Viruses are one of the oldest threats to computers. An infected remote computer can spread viruses quickly to any computer connected to the network.

With the advent of work flexibility such as working from home, virus infection in home computers is becoming common if the computer does not have antivirus protection, or if the antivirus software is not kept up to date.

Consider the impact one infected home computer could have - it could bring down every computer in the network! Organisations should revisit their IT security policy to check whether it includes mandatory installation of good antivirus scanning software on each remote computer connecting to the network. Organisations need to check what assurance they have that virus software runs at all times during VPN connections and how often the IT department uploads corporate computers with the most recent virus definition.

Spyware

Spyware is another threat to VPN and is one of the newest threats to the integrity of corporate networks. A common type of spyware software includes software that displays unrequested advertising everytime we open a website. This sends personal information back to advertisers and tracks website visits. Sometimes spyware is installed on the computer after the employee visits a site, without the user knowing about it. Spyware can affect the performance of infected computers to such extent that those computers are useless for anything other than viewing pop-up ads. The worst scenario is that spyware programs can send confidential and sensitive data to advertisers, hackers or third parties.

Although some tools exist to help manage spyware threats, most remote users are completely uneducated in this area and organisations may be unaware of the threats to the system when employees work remotely. IT management should ask the questions, "What strategies have been implemented to deal with spyware internally and remote computers connecting over VPN?" and "Have any spyware detection and prevention strategies been put in place?"

What to do

Endpoint security is a critical feature of remote access platforms. IT management should:

- revisit policies to see whether they address the different risks posed by remote computers
- ensure that these policies are enforced for all employees, especially senior management who wish to have access to network resources during business travels.

The safety of your VPN is at stake. Your organisation's remote computer security policy should be a priority. If your business does not have effective security measures in place, now is the time to protect your IT functionality.

Tax risk management

GST risk - ATO audit activity

The rate of increase in GST revenues has fallen markedly in contrast to the trend of other taxes, which have shown a strong increase in collections. This may have prompted the ATO's increased GST audit activity, to investigate why the revenue increase has fallen. Are businesses not declaring income? Are they becoming smarter about finding ways of reducing their GST costs or increasing credits? Or are more mistakes being made? Given this increased ATO activity, greater care is needed when dealing with GST to avoid unwelcome attention from the ATO.

Amounts in \$,000s	2001	2002	2003	2004	2005
Total Tax Revenue (State and Federal)	\$214,369	\$217,631	\$238,129	\$257,268	\$278,534
Increase		1.50%	8.61%	7.44%	7.63%
GST %	11.10%	12.60%	13.10%	13.30%	12.70%
GST Revenue	\$23,795	\$27,422	\$31,195	\$34,217	\$35,374
Increase		13.23%	12.10%	8.83%	3.27%

The 2006 budget increased the funds available to the ATO to conduct audit activity. The ATO conservatively estimates that for each dollar spent, four dollars extra revenue will be generated. The ATO has specifically targeted a number of areas for audit activity. In particular, they will scrutinise international transactions to ensure that the GST-free relief is only being claimed when the legislation permits it. The GST-free relief is restricted and is often not available, even when the customer is based overseas. Any business with overseas transactions or overseas affiliates needs to consider reviewing their procedures and the availability of the GST-free relief.

Corporate tax risk management

On 1 May 2006 Second Commissioner of Taxation Jennie Granger outlined, amongst other things, key areas of income tax for large businesses being monitored by the ATO.

These include:

- tax consolidation restructuring - pre and post tax consolidation restructuring, especially those featuring share buy backs and changes in tax residence, large formation cases and groups with larger numbers (or large value) of acquisitions or divestments
- capital management, for example hybrid securities, stapled securities and other financial products, to ensure the debt to equity rules are being correctly applied, and a range of complex financial arrangements where corporate groups seek cross-border tax arbitrage opportunities
- tax payments from the energy and resource sector, and
- intellectual property - the ATO is examining cases where the Australian taxpayer transfers intellectual property to a low tax country and pays insufficient Capital Gains Tax. Cases being scrutinised involve large new international related party royalty fee deductions, and complex financial arrangements around the time of the restructure.

While acknowledging that there has been a stronger emphasis on tax risk management, the ATO still sees audit cases where major transactions and particular interpretations have been put in place which have resulted in significant tax exposures. In some cases, it appeared that the Board of Directors had not been actively involved on potentially big tax exposures. Only after the event had the Board been truly involved in understanding, unravelling and resolving the big tax issues. Ms Granger noted the importance of Boards having an appropriately resourced tax function to keep them well informed of the group's potential tax risks while arrangements are being put in place as well as how those risks are being managed.

Tax risk management

Large business tax compliance

The ATO is currently working with the Corporate Tax Association and accounting firms on the next large business tax compliance booklet. The updated booklet is to be released at the ATO's Large Market Symposium in Sydney this August. The ATO's compliance program 2006-07 will also be released in August.

The new version of the booklet explains the ATO's current compliance approaches, particularly in relation to risk reviews and audits. The aim is to enable a better understanding of how the ATO works with large business and the importance of ongoing dialogue between the ATO and taxpayers to ensure issues are addressed and managed appropriately.

Tax Risk Management

In order to manage tax risks, companies will need to conduct the following:

- compliance reviews - to ensure that issues are historically correct
- systems reviews - of input and outputs, as well as policies and procedures
- preparation and effective implementation of Corporate Tax Plans - the management of taxation obligations, risk and outcomes at the Board level
- review of direct taxes - to ensure compliance with corporate tax and associated areas ie. tax consolidation regime, thin capitalisation regime
- review of compliance with indirect tax laws, eg Goods & Services Tax and other employment taxes, stamp duty, land tax and other withholding taxes
- measures to ensure that any exposures to international tax laws, such as compliance under the controlled foreign company regime, foreign investment fund regime and transfer pricing regulations are appropriately addressed.

If you would like to discuss any of the above information, or any specific issues relating to your organisation, please do not hesitate to contact Shirley Liew or Andrew Rigele.

Grant Thornton

For further information please contact:



Shirley Liew
383 Kent Street
Sydney NSW 2000
T 02 8297 2489
F 02 9299 4445
E sliew@gtntsw.com.au



Andrew Rigele
383 Kent Street
Sydney NSW 2000
T 02 8297 2595
F 02 9299 4445
E arigele@gtntsw.com.au

DISCLAIMER

This newsletter is general in nature and its brevity could lead to misrepresentation. No responsibility can be accepted for those who act on its content without first consulting us and obtaining specific advice.

Grant Thornton (NSW) Pty Ltd is an independent business entitled to trade under the name Grant Thornton. Grant Thornton is a trademark owned by Grant Thornton International and used under licence by independent firms and entities throughout the world. Liability limited by a scheme approved under Professional Standards Legislation.