

# risky businesses

Grant Thornton 

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

## A proactive approach to protecting your IT security

Ignoring difficult issues like IT security does not mean there are no threats to your company's IT security. While lack of questioning may seem an easy option, it's not only self-defeating, it's seriously risky. Security gaps can only be addressed if they are identified.

Management should be aware of the capability of their technology to provide security event information. Can the existing systems detect misuse? If so, are these events regularly reported?

Without periodic reporting, breaches could be occurring without your knowledge. Ignorance of attacks on the company's infrastructure due to lack of records and failures in compliance can make a company incredibly vulnerable. A full IT risk audit can bring you up to speed on the state of your IT security.

### Compliance improves security

Very often, organisations improve security by raising the cost of poor security. Companies spend more money on security, because they don't want to fail an audit. However, having adequate data and documentation rather than a stop-gap, not only supports compliance with control and security, it will help you meet your audit requirements and track control assessments.

Increased regulatory requirements such as the advent of Sarbanes-Oxley Act in 2002 ('SOX') and auditing reforms, and the need for executives to monitor and certify reports and internal controls, often results in valuable managerial resources being taken up by the finer details, instead of being used more efficiently.

These demands are exacerbated by the risk of litigation which must be taken into consideration. Further to this, individual managers are likely to insist on precautions and paperwork that diversified stakeholders would find excessively costly. Whilst these measures ensure compliance are well meaning, given the litigation risk inherent in the certification requirements, it can result in excessive timidity for corporate management. With potentially billions of dollars in liability at stake, the profitable corporations subject to SOX may find executives increasingly focused on anticipating litigation difficulties, rather than business issues!

### What's the answer?

Management should make it clear that compliance obligations are all about business benefits. The focus should be on how compliance can improve business and processes and deliver better speed to market. Compliance should never be seen as a mere checklist. Instead you should consider the reasons these requirements exist and how they can be used to help sustain a competitive advantage.

Self-assessment or risk self-assessment are useful ways to acquire information about business process risks, while empowering the process owners to take responsibility for identifying and mitigating those risks. It helps you identify where you should channel your risk management resources most effectively.

What is needed is strong top-down leadership. CEOs and CFOs must drive a culture of control consciousness, by endorsing, promoting and fostering compliance as the means to achieving improvements in business processes, security and systems improvements. These include more automated controls (preventive), business continuity planning, disaster recovery planning and so on.

Finally - why be reactive and change only when you have encountered a 'near death experience' with the regulator? By being proactive and working out where the regulator is coming from, you will be able to turn what may seem a negative into a positive benefit by adding trust to the equation.

# Outsourcing - A risky proposition?

## Outsourcing does not have to be a debilitating proposition

Increasingly, as companies choose to devote key resources to core business activities, supporting functions are being outsourced. These can range from performing a specific task under the direction of the client to replacing entire business units or functions. In recent years, due to the drive for better cost and risk management, improved service delivery and greater speed to market, there has been a significant increase in the use of outsource service providers for key processes. These often include IT-intensive activities such as information processing, claims management and payroll.

Many of these services affect the client's financial statements. Because of the impact on the user's financial statements, auditors performing audits may need to obtain information about the services, the service organisation's controls, and their effects on the financial statements. To achieve this, compliance-conscious organisations need to take steps to ensure that their service providers:

- document their financial processes
- carry out a risk assessment
- have adequate controls over financial reporting that have been thoroughly tested for effectiveness.

This is the responsibility of the user organisation and should never be delegated to the service provider

## Which providers and functions can this apply to?

Service organisations performing functions that may affect their clients' financial statements include:

- custodian banks
- fund accountants
- bank trust departments that hold and service assets for employee benefit plans or for others
- mortgage bankers that service mortgages for others
- application service providers that provide software applications and a technology environment that enables customers to process financial and operational transactions
- payroll outsourcers
- outsourced data centres
- third party web-hosting of e-commerce and
- customer relationship management databases.

## Controls are needed

The business side needs to develop a management infrastructure to establish and maintain internal controls and ongoing processes that ensure reliable regulatory compliance. IT on the other hand, needs a technology framework that capitalises on existing resources and makes point solutions the exception rather than the rule.

These are important because complex operating models can compromise direct control over an organisation's data and IT systems. Earnings and capital could be at risk from negative public opinion as a result of poor service, disruption of service, or violations of consumer law. This can occur if a third-party's interaction with customers is not consistent with the organisation's policies or standards. It also occurs when there is negative publicity about adverse events involving an organisation.

Risks to earnings or capital may also arise from problems with service or product delivery. An effective business resumption plan and appropriate contingency plans will minimise risk.

If you use service providers you need to ask:

- What outsourced processes may affect your financial statements?
- Has the service provider conducted proper risk assessments focusing on processes, systems and people?
- Does the service provider have effective controls in place to mitigate, eliminate or avoid risks?
- Does your contract with the service provider appropriately address losses?
- Are you comfortable that changes to outsourced processes or systems will not have a material effect on our financial information?

There are two ways to deal with these questions:

1. Have your internal or external auditor conduct an audit of the service provider in question or
2. If the service provider has its own external auditor, require that they provide audit reports to your organisation.

### Auditing a service provider

From the user's perspective, if the company has large control over its outsourced activities, it may need to perform risk and control assessments on the service provider, as well as testing that the controls are effective. The client may use internal or external audit to evaluate the service provider's control environment, as an extension of normal audit procedures.

It is important to determine contractual provisions for financial control auditing and to reach agreement on the audit process between the user and service provider. From the service provider's standpoint, if multiple clients seek audits, their resources could become overloaded by having to provide a range of assurances about internal controls. So it may not be practical for audits to be conducted by the service provider.

### Auditing guidelines

In Australia, Auditing Guidance Statement AGS 1042 "Reporting on Control Procedures at Outsourcing Entities" provides guidance to auditors engaged in reporting on control procedures at outsourcing entities and offers guidance for both the user's auditors and the service provider's auditors.

Service providers may opt for a Statement on Auditing Standards (SAS) No. 70, Service Organisations ("SAS 70"). This is an internationally recognised auditing standard developed by the American Institute of Certified Public Accountants (AICPA). SAS 70 is accepted under SOX (Sarbanes-Oxley Act 2002) in relation to section 404. A SAS 70 audit involves an external, independent evaluation of service provider controls, their execution and effectiveness. The SAS 70 audit addresses critical benchmarks, including completeness, accuracy and timeliness of the control activities and processes.

When originally released, the SAS 70 was intended for use by firms to help them assess controls in place at companies offering services that were being outsourced by that firm. A service provider supplying an outsourced service that materially affected the financial statements of the client firm had to provide a SAS 70 audit document or be subject to an internal controls audit by the client. In the wake of Enron and other similar accounting scandals, it has become widely accepted that firms that act as the processors of transactions (including investment managers) and not merely as record keepers, could be expected by clients and boards to produce a SAS 70 audit report as well.

To remain competitive in the current market environment, investment management firms find it increasingly necessary to document their internal controls in the form of a SAS 70 audit document. For example, take an institutional client conducting an internal controls audit on service providers (such as an investment management firm or mutual fund boards). The client would find itself increasingly responsible for ensuring controls over financial reporting and would therefore ask for the audit documents on a regular basis.

It is instances such as this that the distinction between the two types of SAS 70 audit reports becomes important. While a SAS 70 Type I document only serves to provide an outline of process and an overview of controls at an investment management firm, a SAS 70 Type II, which is far more extensive in its review, is very useful in documenting controls that would normally have to be examined several times a year by different parties. For investment management firms that manage mutual funds, the passing of the SOX Act 2002 and the mandatory implementation of compliance with Section 404 of this act, has made the SAS 70 Type II audit an indispensable document.

### These documents help both parties

With a SAS 70 report, user organisations will not have to conduct their own audit of the service provider's controls. Service providers may use a SAS 70 report for commercial purposes as well. Companies with SOX compliance and provision of a SAS 70 report as a standard offer competitive advantage.

Regulatory-savvy firms have also been able to leverage their SAS 70 document when testing for some of the obligations under Section 404. Section 404 includes an assertion by management that there are effective internal controls over financial reporting. Full documentation of controls, considered significant to the process of financial reporting, is required. The SAS 70 Type II audit affords a strong base for building a full review of controls for use under Section 404. It provides the type of extensive testing necessary to meet the controls requirements under Section 404, and offers a standard for the additional controls testing necessary for a firm's full compliance.

The SAS 70 document is an excellent resource for use in place of internal controls audits conducted by institutional clients, and can be leveraged fully in many other areas of an investment management firm. The information collected and documented in the SAS 70 provides a consolidated source of information for policies and procedures documents and other internal, client, and regulatory requests. However, a full understanding of the limitations, as well as the uses, of the document is essential for an organisation to gain the most from the information collected and the controls that are audited.

Recently, some organisations have required their suppliers to provide a SAS 70 statement, even though the services provided were not outsourced. It is therefore important to determine (by mutual agreement) whether or not the services provided are considered to be outsourced activities. Definitions vary, with most typically defining outsourced activities as those transferred to a third party that otherwise would have been administered in-house.

A key objective when outsourcing is effective risk management, passing as much as possible to the service provider. But the reality is that the risk of financial losses and damage to an organisation can never be fully outsourced. As a user organisation, you remain responsible for ensuring that there are significant controls over the business processes you have outsourced.

# Mergers and Acquisitions: the IT Impact

Mergers and acquisitions (M&A) between two large companies provide opportunities for business and technical consolidation that will allow the combined entity to achieve greater efficiency and economies of scale, however, this is easier said than done.

Merging technical and operating environments is a daunting task fraught with logistical and political pitfalls. Without careful evaluation of the underlying business rules and policies of the two merging entities, the combined company can be burdened with a less-than-optimal operating environment. This can seriously undermine the value of the merger.

John S. Webster of Computerworld projected that in 2010, M&A activity will continue to be an almost everyday occurrence. So the big question is: who will survive the turmoil and how to survive?

## IT is a critical factor

Information technology integration is critical to M&A. Though M&A should produce greater efficiency, it cannot be denied that there are acquisitions that have taken place in which value was not realised as a result of poor or costly integration of IT systems.

Fortunately, there are methodologies that allow businesses to successfully integrate their technical infrastructures and processes, resulting in stronger post-merger market positions.

M&A transactions need to apply due diligence procedures. Prior to an investment being made in a company, IT risks and exposures should be identified for an investor across all business sectors. IT due diligence lets the investor reach an informed IT investment decision by valuing the risk and worth of technology companies, IT departments and IT projects. Both tangible and intangible IT assets are evaluated.

So, what are the IT considerations in M&A?

When considering an M&A organisations need to:

- conduct a fact-find on IT systems, people contracts, strategy and commitments
- determine whether major investment will be needed following the deal
- identify compatibility with acquiring company systems
- assess the robustness and reliability of systems etc.
- evaluate scope for cost savings following acquisition
- decide how these considerations will affect the deal price.

An IT due diligence scope will typically determine:

- the extent of IT infrastructure and operational dependency of any outsourcing arrangements
- the existing relationships between target company and its third party suppliers and any future or ongoing commitments
- fitness for purpose of current systems
- the target's in-house technical skills and capability and its dependence on key personnel
- any future maintainability issues with any existing key application.

Finally, IT management must be prepared and alert to M&A opportunities and threats. They need to be actively involved in all significant business decisions at the earliest possible stage. IT staff should continually build on knowledge, network with peers and keep abreast of global technology developments in their industry.

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@gtnew.com.au



**Andrew Rigele**  
383 Kent Street  
Sydney NSW 2000  
T 02 8297 2595  
F 02 9299 4445  
E arigele@gtnew.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.