

Business risk briefing

Business Risk Services Newsletter Summer 2010

Welcome to the Summer 2010 edition of Grant Thornton's Business Risk Services (BRS) newsletter.

The past few months have been a busy time for BRS, and in the governance and risk fields in general. This is reflected in the diversity of topics in the current edition.

Whilst the media focus on governance in Irish organisations continues unabated, there have been a number of significant developments recently, including the Financial Reporting Council (FRC) issuing an update to the Combined Code on Corporate Governance, and the Financial Regulator issuing consultation paper CP41 on corporate governance in financial institutions.

Our main article overleaf covers these recent corporate governance events, and some highlights of our own work in this area, including the publication of our Corporate Governance Review 2010, the subsequent lively panel debate and Grant Thornton's appearance before the Oireachtas Joint Committee on Economic Regulatory Affairs.

In the field of risk management, we have an introduction to the newest ISO standard on risk management, ISO 31000, and a brief look at its benefits and implications.

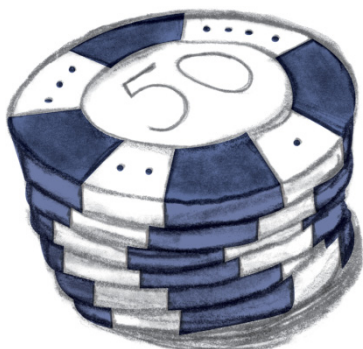
A guest article from VAT specialist Finbarr O'Connell gives an overview of VAT risk, and how internal auditors should be aware of the many

pitfalls, particularly where public sector organisations have recently been brought into scope for VAT.

Finally, an opinion piece from Mark Gahan discusses the concept of privacy—and why it is relevant to all of us.

We hope you find this useful and informative, and we would be delighted to hear your feedback on these issues.

Cian Blackwell
Partner, Business Risk Services



In this issue

Introduction	1
Corporate Governance Review	2
Risk management: ISO 31000	4
Managing VAT compliance risk	6
What's so important about privacy?	9
Grant Thornton contact details	11

Corporate Governance review and further developments

In March of this year, Grant Thornton launched the fourth annual Corporate Governance Review, a report assessing and commenting on compliance with the Combined Code by Irish listed companies.

Although it received considerable media attention in its own right, the timing was opportune given the continuing public disquiet over perceived laxity in governance standards amongst Irish companies.



The Corporate Governance Review assesses the level of compliance amongst companies on the Main Securities Market of the Irish Stock Exchange with their governance framework, the Combined Code on Corporate Governance (‘the Code’).

Whilst this is a relatively small group of companies, it contains many of the largest organisations in the country, including several—such as the major banks and Aer Lingus—with significant state shareholdings.

The report covers a wide range of governance principles and provisions from the Code, including perennial governance topics such as board balance, independence, remuneration, sub-committees, auditing and risk management, and assesses the percentage of companies that comply.

However, rather than focusing merely on the statistics, the report is designed to provide plentiful guidance to companies seeking ways to embrace good governance practice—and those seeking insight into where they may fail to meet an acceptable standard. The guidance can be applied by any organisation, and is relevant to private companies and public sector organisations.

Interestingly, our previous Corporate Governance Review published in March 2009 made many of the same recommendations as the 2010 review. However, the 2009 review was

received considerably less favourably, even prompting some comments that implied the firm’s stance was overly critical for the sake of attracting publicity. The response to the 2010 report—noticeably more favourable—indicates that what has changed since 2009 is not the standards exhibited by Irish companies, but rather the willingness to accept that significant improvements need to be made.

In an effort to contribute and enliven the dialogue on the subject, this year we introduced a new initiative—a panel debate on governance with a range of prominent contributors.

Hosted by Ivan Yates and including Sinead Donovan (Grant Thornton), Kevin Prendergast (ODCE), Howard Millar (Ryanair), Frank O’Dwyer (IAIM), Imelda Reynolds (Beauchamps) and Constantin Gurdgiev (economist and lecturer), the debate covered a wide range of issues—and some strong opinions.

The response to the 2010 report—noticeably more favourable than last year—indicates that what has changed since 2009 is not the standards exhibited by Irish companies, but rather the willingness to accept that significant improvements need to be made.

Among the points made were the following highlights:

- The reputation of the country has been damaged and needs to be repaired internationally
- We should consider adopting the same approach as the US, requiring the CEO and CFO sign off on financial statements and internal controls
- Boards were let down by those who held the information—the information provided wasn't challenged by boards
- The pool of non-executive directors is not as limited as it is perceived—we need to look beyond Ireland to where Irish companies are actively trading
- All companies should put the remuneration committee report to a non-binding 'say-on-pay' vote
- Irish companies do not face a promising future for the next 5 to 10 years unless they can differentiate themselves—corporate governance is an important way of doing this
- Professional investors and fund mergers use contrarian advice, and boards should do so too
- Companies are ticking the boxes on risk and making bad risk decisions—risk committee composition needs to be improved
- If there is one unified regulator, there is a risk that they may focus their resources on particular areas—multiple regulators allow for a broader focus
- The audit 'expectation gap' is a major issue—shareholders expect more of an audit than the scope will allow for; the role of auditors is to say whether the financial statements show a true and fair view, not to judge the company's future risk profile
- It will be helpful to investors if the role of the auditor is changed—expanding the scope to give an

opinion on internal controls, as in the US

- There is no real enforcement of Combined Code, and there will be no accountability unless the shareholders demand it
- There should still be an option to opt out of particular principles of the Code, but the quality of disclosures needs to improve greatly.

Given the topic under discussion, the occasionally controversial and contradictory nature of the debate was reassuring.

The period after the review and debate has seen governance remain firmly on the agenda for regulators, although there is much still to be decided.

The FRC has updated the Combined Code, now called the UK Corporate Governance Code, and although this indicates the end of the current stage of the process for the UK, the Irish Stock Exchange has indicated that they will seek responses from interested parties on how this new code should be applied in Ireland. The changes to the Combined Code are generally not radical, but some have generated debate, including new requirements on directors' terms of office and on diversity in boards. See below for a link to our factsheet on the major changes.

The Financial Regulator is also seeking responses, in this case to consultation paper CP41 on corporate governance. Although this covers only financial institutions, the draft regulatory requirements make numerous suggestions that are relevant to other organisations, particularly public interest entities such as state and semi-state companies, and large private companies.

Finally, we were delighted that Grant Thornton was invited last month to appear before the Oireachtas Joint Committee on Economic Regulatory Affairs to discuss our report and governance recommendations. Paul Raleigh, Sinead Donovan and I presented to a group of interested and well-briefed deputies, and the content of our address is available at: <http://grantthornton.ie/oireachtas>

All of these topics, and many more of relevance to governance, will be discussed on Grant Thornton's corporate governance blog which will be online by the end of June. To receive an update, please register here: <http://grantthornton.ie/cgblog>

Cian Blackwell
Partner, Business Risk Services

The Grant Thornton Corporate Governance Review 2010 can be downloaded at:
<http://grantthornton.ie/cg2010>

Our factsheet on recent changes to the Combined Code, is available at:
<http://grantthornton.ie/cgupdate>



Taking the risk out of risk management: ISO 31000

Over the past two years we have witnessed a contraction of the global economy on a scale not witnessed for over half a century.

The root causes of these events will be analysed and debated for years to come, but some things are clear—notably the fact that many large corporations appeared to be completely unprepared for the circumstances that transpired.

Many commentators have pointed to the relaxation of regulation, particularly in the banking sector, as a primary contributor to the crisis.

It is true that increased regulation might prevent the same problem from happening again in the future. But as we have seen from past experience it is becoming more difficult for individual regulators to keep abreast of the ever changing complexity of the financial services sector. Most banks and other large corporations are now operating globally and on such a large scale that implementing regulations to police these large corporate bodies would be immense and arguably beyond the current regulatory bodies' abilities.

An alternative method for preventing a repeat of this economic meltdown would be to gain an understanding of the root causes and try to learn from the mistakes made in the last 20 years.

In order to achieve sustainable recovery, large corporations will need to change the way they perceive and manage risk.

Now there is a solution which can help

A new International Standard, *ISO 31000:2009, Risk Management – Principles and Guidelines*, was issued in November 2009. It can be used by organisations of all types and sizes to manage risk effectively, under a common framework.

Until November 2009 there was no international standard available to manage risk. Prior to *ISO 31000:2009* being issued the *AS/NZS 4360, Risk Management* standard had been widely used. This was the Australian and New Zealand standard; however since *ISO 31000* has been published Australia and New Zealand have also adopted it and retired the previous standard.

Kevin W. Knight AM, Chair of the ISO working group that developed the standard explains, "All organisations, no matter how big or small, face internal and external factors that create uncertainty on whether they will be able to achieve their objectives. The effect of this uncertainty is 'risk' and it is inherent in all activities."

The standard provides a framework which any organisation can use in order to implement a risk management policy.

"In fact," he continued "it can be argued that the global financial crisis resulted from the failure of boards and executive management to effectively manage risk."

ISO 31000 is expected to help industry and commerce, public and



private, to confidently emerge from the crisis.

How can ISO 31000 benefit your organisation?

This standard has very recently been adopted by Ireland and the NSAI have published a guidance document. The benefits of using the approach outlined in the standard are:

- it avoids organisations ‘re-inventing the wheel’;
 - it allows all to benefit from proven best practice;
 - it provides a universal benchmark;
 - it advises exactly what you need to do and how you need to do it – no wasted effort and no false starts;
 - it is scalable – works for all sizes of organisation;
 - it fits ‘ERM’ requirements, but will also allow silo/project risk management; and
- it adds value and reduces the risk in risk management and helps create value out of uncertainty.

ISO 31000 can be applied in any organisation – small, medium or large, whether they are commercial, non-commercial, voluntary, or in the public sector. This standard will give these organisations a useful and practical tool for integrating risk management into their existing management structure.

The Public Sector

With the publication of the revised Code of Practice for the Governance of State Bodies in 2009, there is a new requirement for boards of public bodies to ensure there is a risk management policy in place.

Implementation of the ISO standard will set out a risk management framework and process that can help address requirements outlined in this document and others such as *Risk management Guidelines for Government*

Departments and Offices – Department of Finance March 2004.

Conclusion

In future, if organisations wish to manage both internal and external (market) risk effectively in order to reduce the probability of failure and as a result increase the probability of success, a comprehensive risk management model needs to be implemented. A fully integrated risk management plan is increasingly used to predict both positive and negative consequences of any particular strategy. It must be integrated into the culture of the organisation with an effective policy programme led by senior management.



Shona O’Hea
Manager, Business Risk Services



George Carroll
Senior Consultant, Business Risk Services

Managing VAT compliance risk

Tax is such a technical area that even at the best of times it requires expert help for most organisations and individuals to ensure optimal compliance. However, VAT legislation has been changing at quite a pace in recent times and although commercial organisations have been affected by VAT for some time, in light of the EU decision regarding Local Authorities and Public Bodies, charging VAT on services becomes relevant to a wider group of organisations.

Whilst previously seen as a technical area best left to tax specialists, we are seeing increasing numbers of internal auditors turning their attention to tax compliance, and VAT is one of the areas identified by many as being high-risk.

In the past six months alone, taxpayers and practitioners have had to deal with:

- an impending change to the VAT status of local authorities and public bodies;
- a change to the place of supply rules for certain services, a new method for reclaiming VAT incurred in other countries, as well as increased compliance requirements for some service providers (all part of ‘The VAT Package’);
- a new margin scheme for travel agents and tour operators (TAMS);
- a new scheme for dealers of second-hand means of transport (and phasing out of the old one);
- a myriad of smaller amendments and ‘tweaks’ to the legislation; and, perhaps the most sweeping change:
- an entirely new system recently introduced to deal with VAT and property transactions.

In turbulent times, it’s important that we don’t lose sight of the basics. VAT impacts virtually all businesses and it can be a significant cost, especially if not dealt with correctly. In our experience, Revenue audits have in recent times become increasingly focused on VAT. In the current economic climate, many businesses will not be operating at a profit. However, VAT is a tax on transactions (not profits) which means that even very unprofitable businesses can incur substantial VAT liabilities. For this

reason, VAT audits are likely to remain as popular as ever with Revenue.

Common VAT pitfalls

Below are some common VAT pitfalls which are frequently encountered during Revenue audits, and internal auditors should be alert to them when examining related processes. These mistakes can easily result in large settlements with the Revenue.

VAT cannot generally be reclaimed on the following items:

- entertainment for clients, staff, personal use etc (Note: VAT recovery relating to business entertainment is currently being examined by the ECJ);
- food and drink (unless acquired as stock-in-trade for resale);
- accommodation (unless at a ‘qualifying’ conference);
- passenger cars (note: 20% of VAT is recoverable on purchase or hire of certain new passenger vehicles used for business purposes); and
- goods or expenses incurred that relate to a VAT exempt activity carried on by the business.

Valid invoices must be received in order to reclaim VAT – these should include:

- date of issue and sequential number;
- VAT number of supplier;
- details of goods/services supplied
- full name and address of supplier and customer;
- invoice amount, VAT rate and VAT amount; and
- VAT in question must be Irish VAT expressed in euro.

Property transactions

Errors in VAT frequently occur where properties are bought or sold or where leases are being granted, assigned or surrendered. It is vital that VAT advice is taken prior to entering into any such transactions, particularly in light of the recent amendments in the legislation in this area.

International transactions

Care must be taken when dealing with cross-border transactions. In many cases, VAT is not chargeable as the invoice will be zero-rated. However, this treatment generally requires that certain conditions are satisfied. It is vital that invoices are not issued without VAT (in error) as the supplier remains liable for the VAT, and possibly interest and penalties. It is equally important not to pay VAT to suppliers (where it is not correctly chargeable) as it may be extremely difficult to recover any such VAT.

VAT rates

Businesses need to ensure the correct rate of VAT is applied to all goods and services supplied. While the standard rate of VAT in Ireland is 21%, the reduced rates of 13.5% and 0% apply to many goods and services and many services are also exempt from VAT. Many businesses make supplies at different rates and this can equally apply where a mixture of goods and services are supplied for a single consideration.



Statistical forms and general compliance

The penalties for a range of offences (including failing to submit VAT returns in a timely manner) have recently been substantially increased. It is therefore important that businesses complete and submit returns on-time. This applies to VAT returns, Annual Return of Trading Details, Intrastat returns, VIES returns etc.

Common VAT opportunities

It is equally important for businesses to be able to identify where VAT savings can be made. In some cases, cash-flow savings can be achieved which may be vital in the current downturn. In other cases, real savings can be made which will impact significantly on the bottom line for the business. Below are some common opportunities which businesses may be able to avail of.

Bad debt relief – can you claim a refund of VAT already paid to Revenue? Many businesses have utilised this relief as debts have become increasingly difficult to collect.

Cash receipts basis – can you account for VAT when paid by your customers rather than when the invoice is raised?

“VAT is a tax on transactions which means that even very unprofitable businesses can incur substantial liabilities...VAT audits are likely to remain as popular as ever with Revenue”

VAT groups – can a cash-flow or real VAT saving be generated by using a VAT group? Real savings can be made where one of the parties is involved in exempt activities and the parties make supplies to each other.

Retained deposits/cancellation fees – can you claim a refund of VAT where a deposit or advanced payment from a customer has been retained but no supply has taken place? This relief is available to more than just hotel operators.

VAT 13B certificates – is 75% or more of your turnover generated from customers established overseas? If so, you may be able to have your suppliers invoice you without charging VAT.

VAT on ‘qualifying’ accommodation in Ireland – can you reclaim VAT incurred on these costs which relate to attending conferences?

VAT on ‘business cars’ – can you reclaim VAT incurred on such purchases? From 1 Jan 2009, this is possible assuming certain conditions are satisfied.

Reclaiming foreign VAT – have you incurred VAT abroad, and can this be reclaimed? From 1 Jan 2010, EU VAT refund claims are made to Irish Revenue who in turn seek the refund from the other country.

Timing of issue of invoices – can you delay issuing invoices to defer the time at which the VAT is due? This may be possible where goods or services are supplied.

Timing of VAT returns – can you submit your VAT returns less frequently if you have small liabilities or more frequently if you are in a continuous refund position?

Review of input tax recovery methodology – should you be reclaiming more VAT? There are many ways to calculate the appropriate percentage recovery (not just turnover basis) and these should be examined.

Large asset purchases or unprocessed supplier invoices – are you reclaiming VAT at the earliest opportunity?

VAT rates applied – should you be accounting for VAT at a lower rate? Suppliers should review whether there are opportunities to reduce their VAT liabilities, particularly where they supply a wide range of goods to persons who do not have VAT recovery for those items.

The above are a selection of the more common pitfalls and opportunities, but there are many others. It is vital that business dedicate time to evaluating their VAT position as this can help to ensure that liabilities are less likely to accrue and may well open up the possibility of some actual savings. It all adds up!



Finbarr O'Connell
Director, VAT

What's so important about privacy?

Data protection, privacy laws, and sensitive personal data are all terms that we're hearing more and more these days.

This is in no small part due to the fact that there have been some high profile cases both in Ireland and internationally where personal data has been stolen or otherwise 'lost'.



But why do you care if some hacker in an obscure region of Russia knows your address, your date of birth, even your PPS number?

Why should you mind if someone from the wrong side of tracks in Beijing commits identity theft against you? They haven't actually stolen your *identity*, you're still the same person. They now merely have some information about you, and the worst case scenario is that they'll try to empty your bank account, which the bank will reimburse you for anyway—right?

Well, not quite, and I think to understand the core of why there is such importance attached to data protection we need to ask ourselves why people feel aggrieved when their personal information is shared without their consent, why people are almost as passionate about the act as the impact.

If you asked a sample of people if they think data protection is important, I'd be willing to bet that close to 100% would say yes, however if you went on to ask them why is it important, I suspect that they'd struggle. They'd have a strong instinct that it is important, that it concerns privacy, but there exists a vagueness about the concrete reasons or impact.

Most of us have an intuitive understanding of what privacy means, and generally linked to this understanding is the concept of dignitary harm.

For example, feelings of guilt, shame, embarrassment, or invasion of privacy may surface if the IT department monitored personal email correspondence between colleagues just because they weren't work related. This is the side of data protection that we find it easy to understand. However, how can we link this understanding of privacy to the example of the Russian mobster or Chinese hacker stealing our bank details or browser history? Where is the guilt, shame etc? They don't appear to exist, so is there more to privacy than protecting our dignity?

Well, there is separate but related aspect to privacy, that of power. Take the example of medical records. Some of us may have no feelings of shame, embarrassment, etc if someone stole our medical records, maybe because you're healthy and have nothing to hide, or maybe you're not healthy but just don't care if someone finds out about whatever condition ails you. However, it is easy to conceive of situations where the theft of personal medial data might

result in both the feeling of ‘dignitary harm’—i.e. the harm that may affect your dignity—and the erosion of power. For instance, in the wrong hands, information about addiction-related illnesses like alcoholism could be used against an individual in a number of ways. Maybe the information will be made public and cause embarrassment, maybe the information will be sold to a health or life insurance company and used as a reason to increase premiums. In these cases the invasion of one’s privacy is manifested as power over somebody.

In fact, privacy and power have been inextricably linked throughout history.

National sovereignty is the power of nations to do to their citizens what they will within the privacy of their own borders (without interference from other nations), balanced by human rights which asserts the privacy of the individual as a counterpoint to the state’s power.

In general, those who have power can define what is and what is not private, they have the luxury of controlling their own privacy while denying that of others. It is no accident that absolute power demands absolute privacy for itself and zero privacy for others. This is a crucial part of how those with power maintain their power and destroy that of others. Think of Germany in the 1930s and 1940s, think of the former USSR, think of any of several dictatorships ruled by despots.

So getting back to the questions raised in the earlier paragraphs, why do we care if some of our seemingly ‘non-dignitary harming’ personal information is stolen or stolen and abused?

“If privacy is outlawed, only outlaws will have privacy.”

Philip Zimmermann

We care about it not because of the information per se, but rather because there is a sense that someone is eroding our sense of privacy and by eroding our privacy they’re eroding our power.

Although there are many people who live in jurisdictions without privacy rights, thankfully we in Ireland—despite what we may complain about—do not live in a totalitarian regime and we do have human rights which protect us.

We also have data protection laws and a Data Protection Commissioner to enforce compliance with these laws.

This does not stop individuals or institutions attempting to circumvent our privacy rights.

There are many so-called ‘attack vectors’ that a thief can use to get his targeted information; these vectors vary from the very technical (e.g. exploitation of operating system or application vulnerabilities on our computers) to simple social engineering (the average computer user is easily persuaded to click on frivolous—but duplicitous—email links, regardless of IT security policies) to common burglary (e.g. a car smash-and-grab to lift a laptop).

Once our privacy has been circumvented, a common goal of the thieves is to turn the stolen information into money, often at the expense of the victim.

However, as an individual you have rights to privacy and data protection. If a thief denies your rights by stealing your personal information, he can go to jail. Earlier this year in the US the leader of a gang of hacker thieves was sentenced to 20 years in a federal prison for the crime of stealing credit card numbers from a variety of businesses. As a data controller or data processor you also have obligations to keep the personal data in your possession secure. If you do not, most western societies, including Ireland, have laws which will punish you for your carelessness. A recent data breach cost Heartland Payment Systems \$12.6 million between fines and expenses.

If you have any concerns about the private data for which you may have responsibility you may want to speak with industry experts. Grant Thornton’s Business Risk Services team can assist you on the practicalities of dealing with this complex—and potentially emotionally-fraught—aspect of modern life.



Mark Gahan
Manager, Business Risk Services

Contact us

Head of Business Risk Services

Tony Thornbury

T +353 (0)1 6805 613

E tony.thornbury@grantthornton.ie

Partner, Business Risk Services

Cian Blackwell

T +353 (0)1 6805 710

E cian.blackwell@grantthornton.ie

IT Audit, Security and Compliance

Mark Gahan

T +353(0)1 6805 878

E mark.gahan@grantthornton.ie

Internal Audit

Tze Mei Li

T +353 (0)1 6805 913

E mei.li@grantthornton.ie

Internal Audit

Shona O'Hea

T +353 (0)1 6805 725

E shona.ohoa@grantthornton.ie

24-26 City Quay, Dublin 2

Offices also in Limerick and Newbridge

This briefing is provided for general information purposes only and is not a comprehensive or complete statement of the issues to which it relates. It should not be used as a substitute for advice on individual cases. Before acting or refraining from acting in particular circumstances, specialist advice should be obtained. No liability can be accepted by Grant Thornton for any loss occasioned to any person acting or refraining from acting as a result of any material in this briefing. Grant Thornton, Irish member of Grant Thornton International, is authorised by the Institute of Chartered Accountants in Ireland to carry on investment business. www.grantthornton.ie





Grant Thornton

Member of Grant Thornton International

Authorised by the Institute of Chartered Accountants in Ireland to carry on investment business.

© 2010 Grant Thornton. All rights reserved.