

# Insurance Evolution

Autumn Edition 2010

Hello, and welcome to November 2010's edition of Insurance Evolution, our publication for the insurance and reinsurance market.

Our financial services group ended the financial year in June with revenues up 13%. What was driving that increase in an environment where revenue growth in our client base was almost certainly not at that level?

You will expect me to say that it was the quality of our people and the excellence of our client services and no doubt they are strong contributory factors. But we were good the previous year too, and we weren't growing at that rate then. I think the main reasons are twofold: regulatory pressure on our client base, and corporate distress.

Regulatory pressure is showing in a number of ways. Some of it is substantive policy change. Most executives in insurance and reinsurance firms will be familiar with the scale of the effort required to be Solvency II compliant, for example. And insurers with exposure to the retail financial services market are having to plan for the effects of the Retail Distribution Review.

Continues on next page →



## Contents

- 01** Introduction from Peter Allen
- 03** Corporate governance
- 06** How much is enough?  
Threshold Condition 4 (TC4)  
and capital for insurance brokers
- 08** Intra-group reinsurance tax update
- 13** Serious data breaches still continue,  
when will organisations learn?

Some of the pressure is thematic: the FSA is currently very exercised with the subjects of client money, and governance, both of which are feeding through to s166 investigations and potentially enforcement action. Some of it is pressure on firms to improve their lines of defence, whether internal audit or the appointment of effective non-executive directors. And, finally, some of the pressure arises from the market in the form of a shortage - in places severe - of appropriately qualified and available resource to help with the work.

Corporate distress has continued to keep us busy, I'm sorry to say. Striking recent examples arising out of the crunch have been the need to re-perform another Firm's audit of a large financial services business to reassure its bankers; and providing actuarial support to the administrators of a substantial insurance group.

Activity in M&A has built back from the very low levels of late last year to something more resembling normality, although the completion rate remains very low by historic standards. We have on a number of occasions completed financial or commercial due diligence exercises recently, only for the deal to stall on price or terms between that point and completion. Buyers remain nervous; vendors hope for improvement.

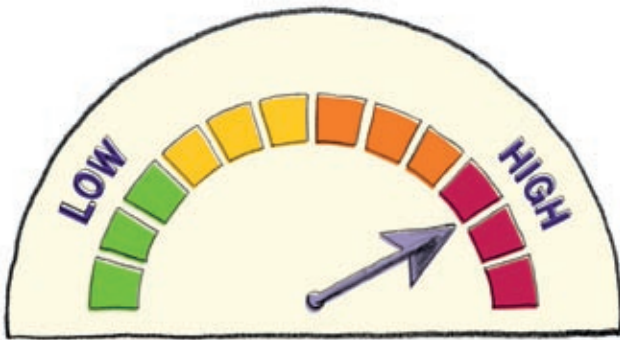
Have a good autumn and do let us know if we can help with anything.



**Peter Allen**

Partner, Head of Financial Services Group  
T 020 7728 2154  
E [peter.d.allen@uk.gt.com](mailto:peter.d.allen@uk.gt.com)





# Corporate Governance

Whilst not the only weakness contributing to the financial crisis, poor governance is certainly widely seen as an important factor. As a result, corporate governance practices have been, and remain, a key topic of focus for UK regulatory bodies and there is also considerable attention being applied internationally. For example the Bermuda Monetary Authority has recently issued a Code of Conduct for insurers which contains extensive provisions relating to various governance mechanisms.

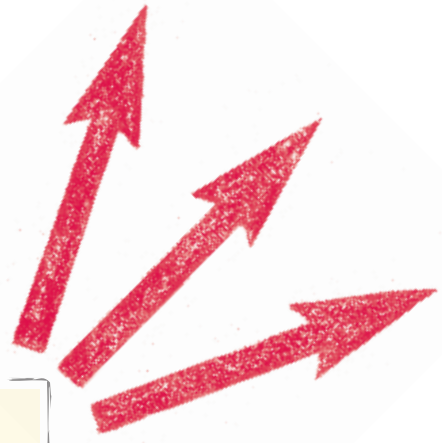
Recent activity has included the Financial Services Authority (FSA) increasing its supervisory intensity in this area, HM Treasury commissioning the Walker review and the Financial Reporting Council producing the new Corporate Governance Code (as a replacement of the Combined Code).

A clear message for all firms is not to assume that because the company may have appeared to function well in the past by producing good financial results with low staff turnover, it will follow that the governance structure remains sound and relatively free from potential risk. A number of firms have been surprised by the findings of an objective review.

As a base point, all companies should of course be headed by an effective board which has collective responsibility for the performance and success of the company. In providing leadership within a framework of effective controls, there should be adequate assessment of risk and its coherent and effective management. The board also has responsibility for

setting strategy and working towards an agreed business plan with appropriate resources being provided.

Additionally boards of directors should be balanced so that there is representation of all functions and disciplines rather than perhaps an overwhelming dominance of sales. Boards should also be democratic in that all members should be given equal opportunity to contribute and that nobody is allowed to dominate proceedings or unduly influence decisions. All board discussion should be subject to challenge which is a fundamental responsibility, particularly of non-executive directors.



### The FSA's approach

The FSA is currently pursuing a strong corporate governance theme in all ARROW reviews and this is supported by Policy Statement (PS) 10/15 which has amended the Approved Person regime and defined more specifically the role of non-executive directors (NEDs). Approved Person responsibility is becoming more acute and, as will be seen from FSA enforcement reports, there have been some swingeing fines issued to individuals.

In addition, the FSA approval process for new non-executive appointees is now far more rigorous, and in some cases, applications to the FSA have either been subsequently

withdrawn by the applicant firm or rejected by the FSA.

Once appointed specific roles should be allocated to all NEDs dependent upon their experience and skills, and these should be supported by a documented role description. This should include a minimum time commitment, a full description of responsibilities, a requirement to keep up to date with relevant management information (MI), a thorough understanding of the current strategy, oversight of performance against the business plan, up to date knowledge of the market in which the firm operates and a working appreciation of financial reporting.

### The Walker Review

In 2009 Sir David Walker was asked to lead a review of corporate governance in the UK banking industry. His original terms of reference referred only to banks but were subsequently extended to identify where his recommendations were applicable to other financial institutions.

The recommendations contained in his final report addressed a wide range of governance issues and the FSA has embraced them enthusiastically. We have referred earlier to the increased focus on

governance within the ARROW risk assessment process, the proposed amendment of the Approved Persons regime, and the Significant Influence Function (SIF) interview process. In addition the FSA is proposing to issue guidance in its Senior Management Arrangements, Systems and Controls (SYSC) sourcebook on the desirability of the appointment of Chief Risk Officers within major insurance companies and the establishment of board risk committees.

### Evidence of change

In recent times we have witnessed significant changes in governance attitudes and styles. There has been a gradual adoption of good corporate practices amongst many medium sized firms and some smaller entities, although there is still considerable work to be done by some firms who continue to bury their head in the sand.

In the insurance broking fraternity, for example, the historic practice of appointing key business producers and 'owners' to the board merely because of status demands and as part of retention packages, has gradually waned, although examples still exist.

---

This has to be a welcome change as some of these appointees adopted an insular attitude and contributed little to the broader responsibility of the board. An additional negative feature of such arrangements was that boards tended to be very imbalanced with a predominance of bullish business developers who sometimes lacked the wider strategic insight and general management expertise demanded of board members today.

---

Most companies have now adopted a far more structured and balanced approach where all the key functions are represented, including compliance, risk, HR and IT. Overall there are more structured frameworks and less emphasis on personalities. Better corporate governance is being embedded into business practice. These companies should now be more efficient and effective and far better equipped to deal with current business issues and increasing compliance and governance requirements, although standards of governance are an ever moving target and firms should continue to review their practices in this area.

### Work to be done

From our experience the key areas requiring most attention are generally better balanced boards with directors taking full corporate responsibility, stronger and more NEDs, greater challenge (and evidence thereof) and robust succession planning for executives. Board MI still tends to be either inadequate in that it reports activities without indicating necessary action or opinion, or alternatively it is too voluminous with key messages lost within minutiae, and directors having insufficient time to absorb all that is presented.

Of course it is not merely sufficient for a board to receive good quality MI but it must be seen to be acted upon and form part of decision making. What action does the board take and is it recorded? Treating Customers Fairly (TCF) data and reports are perhaps a good example of this where boards receive details of complaints and product shortcomings, but there is not always apparent action taken or evidence of sufficient consideration at the highest level.

### Don't rest on laurels

For those companies that have risen to the challenge of robustly rethinking their governance arrangements and taking remedial action, the requirements continue. Annual reassessments of board and main committee effectiveness should be undertaken with perhaps an independent opinion every third year - indeed this is becoming essential for larger organisations.

The performance of NEDs should be reviewed at periodic intervals to ensure that they maintain an up to date and sufficiently extensive knowledge of the business, with training and support from the business where knowledge and skills need to be enhanced. Non executive appointments should also be refreshed at appropriate intervals to maintain independence.

Critical reviews of corporate governance will be with us for some time to come and if done well they can provide valuable, objective guidance and assistance. Good corporate governance should be good practice requirements that work well for the company concerned. Furthermore, good corporate governance theory will only be manifested in practice if it is in tune with the business model.



**Jonathan Houston**  
Senior Manager  
T 020 7728 2227  
E jonathan.houston@uk.gt.com



**Stuart Howard**  
Senior Manager  
T 020 7728 2109  
E stuart.howard@uk.gt.com



# How much is enough?

## Threshold Condition 4 (TC4) and capital for insurance brokers

The banking crisis of the last few years has led to a greater regulatory focus on capital models and solvency of financial services business in the UK, including that of insurance brokers.

---

### **It's all the banks fault isn't it, so why are insurance brokers being targeted?**

Up until a few years ago it was largely accepted by regulators, governments and rating agencies that capital models of firms within the banking sector were sound. How wrong this turned out to be and the banking crisis which followed almost led to the complete collapse of economies around the world.

The fallout of the last few years continues to be felt, none more so than within the regulators themselves who

are currently undergoing significant change and restructure. Lessons continue to be learned, particularly that if something appears too good to be true, then often it is.

---

**As a result, whilst a great deal of focus remains upon the banks, attention is also being turned to other areas of the financial services marketplace to determine whether capital models are sound and therefore whether risk of a similar crisis exists.**

---

For insurance risk carriers, regulatory capital continues to be driven at a European level through Solvency II. No such directive exists for brokers, therefore regulatory capital requirements are driven at a more local level. In the UK, regulatory capital requirements for brokers is articulated through the FSA rules contained within MIPRU 4 (previously PRU 9), and by both Principle 4 and Threshold Condition 4 (TC4) of the FSA Handbook.

## The FSA's response

The FSA's response to these concerns and issues continues to be proactive. Notably, a TC4 Dear CEO letter was sent to all insurance and mortgage intermediaries during February 2010, following hot on the heels of the client money Dear CEO letter sent in January 2010.

The TC4 Dear CEO letter stated that the FSA were concerned that insurance brokers were not paying sufficient attention to the threats of financial viability of their firms, and failing to consider financial resources properly.

The threats of financial viability are of particular importance against an economy which generally remains challenging and the continued 'soft' insurance market which, in the absence of a major catastrophe, looks to remain this way in the near future. As such, the continuing pressure on the top income

line for brokers, the squeeze on margin and working capital for many firms, and the continued restriction on obtaining financial resources from the capital markets, continues to cause concern both within the market itself and with the regulator.

As a result, the Dear CEO in February 2010 letter required firms to undertake a "TC4 assessment" and provided detail of specific points to be considered. Put crudely (and arguably pessimistically), this approach by the regulator could be considered as 'Solvency II for brokers' since the ethos is for firms to align their capital resources to their business risks. It also highlights the limitation of the regulatory capital rules contained under MIPRU 4 which essentially only consider size as a business risk through the straight lime method of calculating capital resource requirements.

## Ok, so what should firms do in relation to this 'TC4 assessment'

Firstly, it is important to understand what TC4 means. Per the FSA handbook TC4 states:

*"The resources of a person concerned, must in the opinion of the FSA, be adequate in relation to the regulated activities that he seeks to carry on, or carries on"*

Put simply firms must maintain adequate (i.e. sufficient quantity, quality and availability) financial and non-financial resources. It is common sense! Such resources may include capital, provisions against liabilities, holdings of or access to cash/liquid assets, and human resources. In addition, it is crucial for firms who are part of groups to consider group risks, particularly the impact of intercompany balances and crystallisation of group liabilities. Finally, any contingent liabilities e.g. E&O claims should also be considered as part of capital modelling under TC4.

Whilst a TC4 assessment will tick the regulators box, moreover it should be considered as being beneficial in terms of useful management information for firms both now and in the future. Therefore TC4 should be embedded within ongoing financial and operational planning and reporting.

Good TC4 assessments are directly aligned to the business plan of firms and provide executive management with valuable information regarding the financial impact of the key business risks and scenarios which, in turn, can support in the development and targeting of key controls or action plans to prevent or address such risks and scenarios.

As a result, good TC4 assessments essentially provide a 'stress test' of the business plan and business objectives, to determine whether current or planned resources are able to support the achievement of the business plan and objectives. The assessment should identify gaps which can then be addressed by management in good time before such gaps lead to significant risk and, in the worst case scenario, failure.

*How much is enough is therefore subjective and differs for each firm. Aligning capital to business risk, as required under TC4, will provide a realistic picture of the required resources to meet the current and future business plan and objectives, and to support in the ongoing viability of individual firms and the marketplace as a whole.*



**Chris Gagg**

Director

T 020 7728 2456

E [chris.gagg@uk.gt.com](mailto:chris.gagg@uk.gt.com)



# Intra-Group Reinsurance Tax Update

For a long time international insurance groups have used intra-group reinsurance as a risk and cost management tool, providing a mechanism through which to pool group risks and allow operating subsidiaries greater capacity and capital strength by leveraging the credit rating of the holding company balance sheet. Indeed, many of the large European and global insurers have such structures in place.

Reinsurance subsidiaries are often located in territories with low tax rates and for this reason tax, rather than the commercial factors mentioned above, is frequently assumed to be the primary driver for the use of intra-group reinsurance. This scepticism from Revenue authorities, combined with the global need to shore up tax revenues and raise funds to tackle fiscal deficits, has led to greater scrutiny of international group structures and a number of proposed tax measures. In this article we highlight some of the key issues associated with intra-group reinsurance for international insurance groups which are likely to be a driver for future structural change.

## **Transfer Pricing**

Transfer pricing rules require that transactions between related parties need to be (and must be shown to be) priced on an 'arm's length' basis. The expectation has been that Revenue authorities would use these principles to challenge the pricing of intra-group reinsurance arrangements. However, reinsurance is a complex business transaction. It involves greater diversity of risk, both in terms of the geographical

coverage and combinations of insured lines, than direct insurance business and the uniqueness of each portfolio of risks means it cannot be treated as a commodity for which a price can be easily established. This complexity together with a perceived lack of transparency has, until a recent case before the Courts, meant that some fiscal authorities have displayed a lack of knowledge about the role and pricing of reinsurance.



DSG Retail Limited (DSG) versus HM Revenue & Customs (HMRC), decided on 23 April 2009 was only the third ever transfer pricing case to be heard in the UK. It represents a landmark decision, being the first in the UK to discuss in detail the appropriate methodology for a transfer pricing adjustment and provides an insight into how the UK Courts and HMRC will apply UK transfer pricing legislation to determine the correct pricing method. Moreover it is perhaps evidence that HMRC's dedicated transfer pricing group is taking an increasingly active approach to transfer pricing. Of particular relevance to the insurance sector will be that the case concerned the captive insurance operations of DSG and showed a detailed understanding on the part of HMRC as to how an insurance premium is priced. The case provides evidence that the investment HMRC has made in understanding the insurance sector is paying off and, as such, it would not be

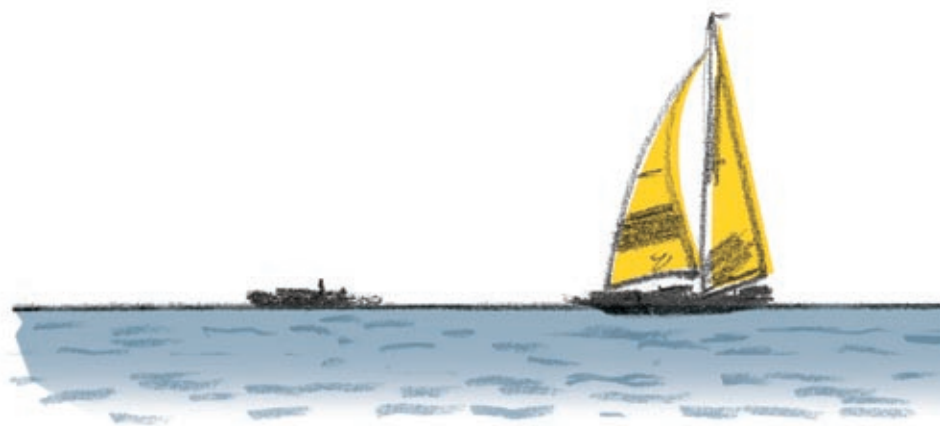
unreasonable to anticipate further challenges of this nature in the future.

The DSG case reinforces the need to prepare and maintain robust transfer pricing analysis. In particular, DSG argued for the use of comparable uncontrolled prices derived from market research, which indicated that the premiums paid fell within an acceptable arm's length range. However, pricing by reference to other reinsurance contracts quickly tends to run into problems over comparability since no two books of business are the same. In the DSG case, HMRC rejected the comparables on the grounds they contained differences such as market conditions and product differences for which reliable adjustments could not be made. Eventually it was decided that, as no suitable comparables could be identified, the profit split method was the most suitable pricing method available whereby an arm's length return on capital for the captive was determined with residual profits allocated to DSG.

---

In terms of scale, the pricing of intra-group reinsurance tends to be the largest and most complex transfer pricing issue for insurance groups and they should ensure that their existing approach to pricing takes into account the conclusions in this case. In addition, it also reinforces the importance of performing a sound economic analysis of commercial arrangements.

---



## **Federal Excise Tax (FET)**

Few tax issues facing non-US insurers have caused quite such confusion as the United States (US) FET. The US has imposed FET for many years on certain insurance and reinsurance contracts issued by foreign companies where some or all of the risks are within the US. It is imposed at a rate of 4% for direct property and casualty insurance and 1% for direct life insurance and contracts of reinsurance. However, certain US double tax treaties exempt premiums from FET when they are received by (re)insurers resident in those treaty countries (subject to certain qualifications).

Whilst it might be thought that FET should apply only to the first transaction (the domestic to foreign link) in the chain, the internal Revenue Service (IRS) has historically taken the view that FET is a 'cascading' tax that could apply each time a US risk is insured and reinsured by a series of foreign companies if the reinsurer is not able to benefit from protection under a suitable double tax treaty. The IRS reaffirmed and formally adopted this position in Revenue Ruling 2008-15 issued in March 2008.

The tax is an openly protectionist measure by the US, based on the perception that US domestic insurers operating within the US tax net are at a disadvantage as compared to non-US insurers, who may be operating out of low-tax jurisdictions. Also, as FET is a tax on premiums rather than profits this can have a significant impact on the profitability of a business.

The imposition of FET on a cascading basis raises a number of issues with which foreign (re)insurers struggle. The most basic matter being that of the IRS's jurisdiction over companies with no US nexus. Indeed, even where a company has entered into a FET Closing Agreement<sup>1</sup> or has signed up to the Voluntary Compliance Initiative issued at the time of the Ruling, applying FET to the second (or any subsequent retrocession) outside of facultative and proportional reinsurance will cause difficulties for taxpayers and the IRS alike as they struggle to determine which premiums relate to US risk and are subject to FET.

Commentators have long disputed the IRS position that FET is a cascading tax; however, the IRS remains confident in its own analysis unless or until the matter is settled through litigation. Indeed, it is possible we will see litigation on this issue in the future as the IRS intensifies its focus on FET compliance.

FET presents a problematic issue for non-US insurers underwriting US situs risks and such insurers face the difficult decision regarding the extent to which they comply with the IRS view of the world. The protection of a double taxation treaty may help to mitigate the impact and as a consequence (re)insurers may choose to redomicile to or route business through jurisdictions such as Switzerland and Ireland where treaty protection is available.

## **Neal/Obama Bill – Limiting Tax Deductions for Foreign Affiliate Reinsurance**

In July 2009 Senator Richard Neal introduced to the House of Representatives a Bill (HR 3424) which would limit the deduction taken by a US insurance company for reinsurance premiums paid to foreign affiliates not subject to US tax. The purpose of the Bill being to address the concern that intra-group reinsurance is being used to shift profits from the US to low/no tax jurisdictions, creating a competitive advantage for US subsidiaries of foreign groups. A similar Bill (HR 6969) was introduced by Neal in September 2008 but expired before the House took action on it.

The Neal Bill had no co-sponsors and was languishing in committee, but the idea was given fresh legs by President Barack Obama by the inclusion of a similar pitch in his 2011 budget proposal. The Neal Bill would, in general terms, disallow tax deductions for 'excess reinsurance premiums' - an amount calculated by reference to an 'industry average percentage', by line of business, based on premiums paid to unrelated parties by US companies.

The Bill makes no distinction as to whether the recipient of the intra-group reinsurance premium is located in a low-tax jurisdiction or otherwise. The Obama proposal is similar in many respects; however, it seeks only to disallow a tax deduction if the reinsurance exceeds 50% of the underlying business- a generally higher threshold than that which would arise under the Neal Bill.

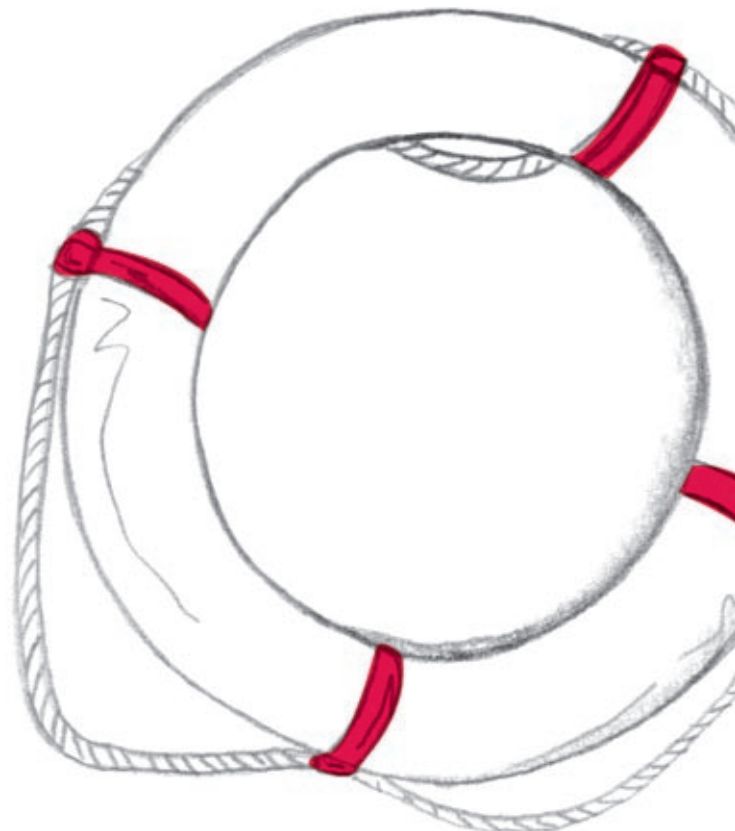
The two proposals have strong advocates and opponents. They are strongly backed by the Coalition For A Domestic Insurance Industry ([www.coalitionfordomesticinsurance.com](http://www.coalitionfordomesticinsurance.com)) which represents 13 US insurance groups and is headed by William Berkley, Chairman of the WR Berkley Group. The Coalition claim that the legislation would close a tax-loophole that benefits foreign controlled insurance companies and affords them a significant advantage in attracting capital to write US business, levelling the playing field for US domestic insurers.

A number of insurance companies and risk managers have joined together to oppose the legislation. The Coalition For Competitive Insurance Rates (CCIR) ([www.keepinsuranceratescompetitive.com](http://www.keepinsuranceratescompetitive.com)) claim that the proposed legislation is protectionist and discriminatory, going against tax treaties. They claim the measures would lead to increased insurance rates charged to US companies and that ultimately this would be passed on to consumers.

The CCIR has commissioned a number of reports to provide evidence that the proposals should be rejected. The most recent was prepared by the Brattle Group and was released in July as a follow-up to their original study produced in 2009. The report concludes that the enactment of the Neal Bill would have the following impacts:

- the supply of reinsurance capacity in the US would reduce by 20% or more
- the market for primary insurance supply would drop, and prices would rise, by 2.1–2.4%
- US consumers would, on average, have to pay \$11–\$13 billion more a year for insurance while at the same time total insurance coverage would fall 4 to 5%
- reduced supply and higher prices would fall disproportionately on those states most vulnerable to catastrophic losses, such as California, Florida, New York, Louisiana, and Texas

The battle lines were drawn recently at a congressional hearing on 14 July before the Subcommittee on Select Revenue Measures of the House Ways and Means Committee over the two proposals and it remains to be seen whether Congress will indeed impose this tax on overseas (re)insurers.



## Conclusions

Intra-group reinsurance plays a vital role in effective management of capital and risk for international insurance groups. The impact of the tax measures discussed above will require groups to examine and question the markets in which they do business and how the group is structured. It is possible we may see an acceleration of the redomiciliation of groups operating out of so-called tax havens to territories which are perceived more favourably and offer a wider tax treaty network. An example of which was seen when

XL shifted their place of incorporation to Ireland from the Cayman Islands, their Chief Executive Officer, Michael S. McGavick, said in a corporate statement : “We believe that our redomestication to Ireland will offer us opportunities to reduce certain risks and reinforce our reputation across our global business platforms”. There is little doubt that the uncertainty around tax will have been one of the ‘risks’ the group will have been seeking to address.



---

### Ian Woodruff

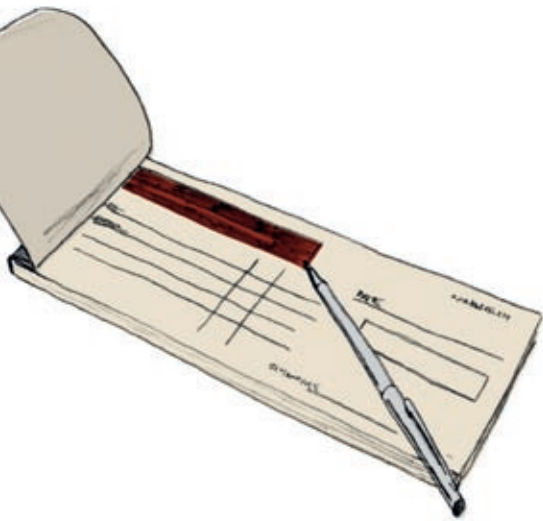
Associate Director

T 020 7865 2189

E [ian.woodruff@uk.gt.com](mailto:ian.woodruff@uk.gt.com)

1. In order for a US payer of premium to be relieved of any liability to pay the FET on premiums paid to a non-US (re)insurer, the IRS generally requires that the foreign insurer obtain a FET Closing Agreement. By entering into an FET Closing Agreement, the foreign insurer agrees to submit to audit by the IRS, file quarterly FET returns ‘as a US taxpayer’ on which they self assess any FET due and provide a letter of credit in favour of the IRS.

# Serious data breaches still continue, when will organisations learn?



Yet another serious data breach has resulted in the highest single fine to date of £2.3m imposed by the FSA to Zurich Insurance for losing an unencrypted data backup tape containing 46,000 customer records. Indeed the FSA said it had taken a third off the fine because Zurich agreed to pay at an early stage - the company would otherwise have had to pay £3.25m.

The FSA stated that Zurich had no effective data protection systems in place or processes to manage the risks to “the security of customer data resulting from the outsourcing arrangement with Zurich South Africa Limited”. Even more worrying was that the actual incident took place in 2008, and it has only just come to light.

Data security breaches are one of the biggest fears that organisations face today, and pose a serious business threat. In recent years, an increasing number of high-profile data security breaches have made headlines.

These events can not only expose a business to costly and potentially devastating legal ramifications, they also can severely damage brand and reputation. High profile data breaches in recent years include:

- HM Revenue & Customs leaked 25 million child benefit records on two CDs that contained names, bank account details, NI numbers, and addresses of people who were in receipt of child benefit in 2007.
- The Financial Services Authority (FSA) fined The Nationwide Building Society £980,000, in 2007, for failing to manage its information securely after the theft of a laptop that held unencrypted data on over 11 million customers.
- In 2009 the FSA fined HSBC Group over £3m for failing to properly look after its customers’ information and private data.

Many firms often decide not to report data breaches to the Information Commissioner's Office (ICO) as they are not obliged to under the current UK Data Protection Act, 1998, although legislation in several other countries and certain individual US states does require this. However, it is very clear from recent cases that these organisations could suffer retrospective punishment if and when they are found out. Are they taking a calculated risk that any breaches will not be discovered? Are they wrongly relying on the current law that it is not mandatory to report data breaches? It could be argued that these

are false assumptions, and there is clear evidence that when they are found out, the fines are likely to be even more severe. Apart from the FSA, the ICO's teeth have recently been sharpened, and the Information Commissioner can now impose a penalty of £500,000 for a data breach under the UK DPA. This remains under review and many specialists in this area believe that the ICO's powers will be further strengthened over the next two years to allow for unlimited fines.

There are current initiatives to introduce mandatory reporting of data breaches for all ISPs and telecom

companies by May 2011 under the EU Data Protection Directive, and this will be extended to all other organisations by 2014. In addition, Article 23 of the EU directive calls for compensation for damage suffered by anyone as a consequence of a data breach which includes any kind of damage, such as emotional distress or loss of reputation. We can therefore envisage that it is highly probable that data breach incidents in the future are likely to get very litigious, and with significant complications because of the chain of individuals, organisations and their third parties who are likely to be involved.

## Data Loss Breaches cost UK businesses an average of £1.68m per incident

Poneman Institute Research, 2009

### So what's the answer?

The best solution is to have good data privacy and management practices in place from the start, to avoid these pitfalls. Organisations need to reduce the risks associated with exposing customer data, losing intellectual property, or violating compliance obligations, and so must evaluate their specific vulnerabilities for each loss area and respond appropriately. A holistic Data Loss Prevention (DLP) programme requires appropriate governance framework and prevents confidential data loss by:

- Embedding an on-going risk assessment programme to manage data security.
- Monitoring communications going outside the organisation.
- Implementing appropriate Privacy Enhancing Technologies such as DLP tools and encryption of data such as laptops, desktops, data storage, USB devices, backup tapes and emails containing confidential content.
- Enabling compliance with global privacy and data security mandates and directives.
- Securing outsourcing and partner communications.
- Protecting intellectual property.
- Preventing malware-related data harvesting.
- Enforcing acceptable use policies.
- Providing deterrents for malicious users.
- Auditing overall compliance through Internal and External Audit functions.
- Delivering an on-going security education and awareness programme.

### Governance framework



### Key questions to ask:

- Is the tone at the top right – are your board members and C-level executives aware of data breach issues and the ramifications of a data breach incident?
- Does your on-going risk assessment process include data loss risks?
- What is your confidential data – do you classify your data?
- Where is your confidential data logically and physically stored?
- How is your confidential data being handled?
- How do you manage confidential data with third parties and outsourcing partners?
- How are the risks of data leakage or breaches minimised in your organisation?
- Do have a DLP programme in place and how do you manage oversight?
- Does Internal Audit have DLP requirements in their Audit Plan and do you have the right skills to audit compliance and maintain a compliance scorecard?



**Yag Kanani**

Head of Security & Privacy Services

T 020 7865 2619

E [yag.kanani@uk.gt.com](mailto:yag.kanani@uk.gt.com)



© 2010 Grant Thornton UK LLP. All rights reserved.

'Grant Thornton' means Grant Thornton UK LLP,  
a limited liability partnership.

Grant Thornton UK LLP is a member firm within  
Grant Thornton International Ltd ('Grant Thornton International').  
Grant Thornton International and the member firms are not  
a worldwide partnership. Services are delivered by the member  
firms independently.

This publication has been prepared only as a guide.  
No responsibility can be accepted by us for loss occasioned  
to any person acting or refraining from acting as a result of  
any material in this publication.

**[www.grant-thornton.co.uk](http://www.grant-thornton.co.uk)**

B1642914