



Advisory


**Financial Services**

**Is your confidential data at risk?**

March 2010

# More and more incidents?

### Bankdaten-CD aus Luxemburg angeboten



(dpa) - Die Jagd nach deutschen Steuerhelfern weitet sich auch auf Luxemburg aus. Steuerhelfern in Bayern wurden jetzt offenbar Daten von deutschen Kunden einer Luxemburger Bank angeboten, berichtet der "Spiegel". Das Angebot werde derzeit geprüft, bestätigte die bayerische Staatskanzlei in München.

Die Entscheidung über den Erwerb liege beim bayerischen Finanzminister Horst Seehofer, hingewiesen, dürfte, wenn die rechtsstaatlich worden seien.

Nach "Spiegel" es sich um Daten kleineren Bank in der Schweiz sowie eines Geldinstituts aus Luxemburg sollen Daten von mehr als 1000 deutschen werden sein. Staatskanzlei und Finanzministerium in München nicht äußern. Auch Baden-Württemberg liegt ein Kaufantrag vor.

Foto: Marc Willwert

**Deutsche Steuerhelfer haben offenbar ein Angebot für eine CD mit Bankdaten aus Luxemburg vorliegen.**

### German bank clients declare assets after data scare

Thu, Feb 11 2010

FRANKFURT, Feb 11 (Reuters) - More than 130 bank customers in Germany have declared previously undisclosed assets following reports that client data has been breached on a stolen CD, tax authorities said. German clients acted after reports that they had been offered a CD with their names and addresses which could yield 100 million euros if they agreed to avoid criminal prosecution. However, the names have not yet been discovered.

*Reputation is one of the key assets of a company*

### German tax cheats rush forward after Swiss CD: report

February 16, 2010 - 7:14AM

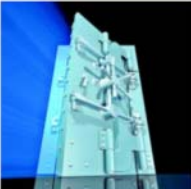
German tax evaders have been giving themselves up in droves after authorities said they would buy a secret disc with the names of up to 1500 people hiding cash away in Switzerland, a financial newspaper says.

According to the finance ministry in the southern state of Bavaria, cited by the Financial Times Deutschland on Monday, more than 270 tax cheats have come forward in one week in that region alone.

### Diskretes Treffen in Senningen

Die Finanzminister der deutschsprachigen Länder debattieren über das Bankgeheimnis

Marianne Truttmann (Brüssel)



Auf Einladung des luxemburgischen Finanzministers Luc Frieden treffen sich am Sonntagabend im Schloss Senningen die Finanzminister von Österreich, der Schweiz, Deutschland und Liechtenstein. Ihre Interessen am Bankgeheimnis sind alles andere als harmonisch.

Diskretion statt Kommunikation gilt für das informelle Treffen der deutschsprachigen Finanzminister, die sich am Sonntagabend im Schloss Senningen versammeln werden. Das passt zum mit Sicherheit zur Sprache kommenden Bankgeheimnis. Mit seinen Kollegen Josef Pröll (Österreich), Hans-Rudolf Merz (Schweiz), Wolfgang

### Conflit fiscal: la Bavière étudie l'achat d'une liste de données

La Bavière a elle aussi reçu une offre d'informations sur d'éventuels fraudeurs de fisc. Les autorités examinent pour l'instant la possibilité de faire l'acquisition de ces données, a confirmé la chancellerie du Land allemand à l'agence de presse DPA.

Le chef du gouvernement bavarois Horst Seehofer a souligné que cela ne se ferait que si ces données ont été acquises de façon légale. Selon des informations du magazine "Der Spiegel", il s'agirait d'informations sur des clients de deux banques en Suisse et au Luxembourg.

Vendredi, on apprenait dans la presse allemande que le gouvernement du Bade-Wurtemberg avait lui aussi reçu une offre de ce type. Mais la coalition CDU/FDP au pouvoir ne s'entend pas vraiment sur la réponse à donner. Le ministre de la justice Ulrich Goll (FDP) ne supporte pas l'idée de "faire un deal avec des voyous".

(ats / 07 février 2010 12:17)

*Majority of breaches go unreported*

### Tax data sale chills Swiss-German ties further

By Gerrit Weismann in Berlin and Haig Simonian in Zurich  
Published: February 6 2010 02:00 | Last updated: February 6 2010 02:00

Every evening on German television the ebullient Jörg Kachelmann forecasts the nation's weather. But Germany's favourite Swiss celebrity is talking about political climates when he says: "We are seeing deepest winter, and how long it will last I can't forecast."

A wintery chill has descended on relations between the Swiss and German governments after Berlin said it was ready to spend €2.5m (\$3.4m, £2.2m) on a CD full of stolen Swiss bank data - records that could generate hundreds of millions of euros in arrears and fines from tax evaders.

### Spiegel ONLINE

08. Februar 2010, 09:33 Uhr

Späte Information über Datenklau

**Gericht spricht Steuerhelfern Schadensersatz zu**

Ein Liechtensteiner Gericht hat einem Kunden der Fürstebank LGT einen Anspruch auf Schadensersatz zugestanden. Die brisante Begründung der Richter: Das Institut habe den deutschen Steuerhelfer zu spät über den Diebstahl seiner Kontodaten informiert.

München - Eine frühere Tochtergesellschaft der Liechtensteiner Fürstebank LGT muss ihrem deutschen Steuerhelfer Entschädigung zahlen, weil sie den Anleger zu spät darüber informiert hat, dass seine Kundenkonten und die von mehreren hundert anderen Bundesbürgern gestohlen worden waren. Wie die "Süddeutsche Zeitung" berichtet, verurteilte der Richter die Rechtsnachfolgerin der LGT Treuhänder zu einer Zahlung von 7,3 Millionen Euro.

For, ignored calls from Doris Leuthard, Swiss president, not to buy "stolen goods". Her decision, backed by the tax authorities, has raised tensions over other issues. Mr Kachelmann says there is a perception that "German politics has taken a step back in Switzerland". Past German leaders refused to negotiate with criminals, he argues.

In Germany and 6m German-speaking Swiss, the bulk of multilingual Switzerland, have become increasingly aware of the situation. The Swiss government has asked the European Union to make it easier for foreigners to work in Switzerland. Since then, the number of Germans in Switzerland has risen to 250,000, a trend that has provided fertile territory for anti-German sentiment.

*People are the weakest link in the security chain*

*Ultimate responsibility lies with Top Management*

# The Information Technology Perspective

## Information Technology

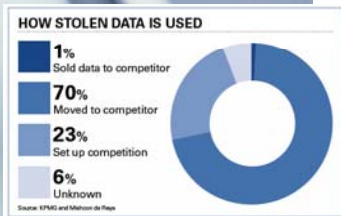
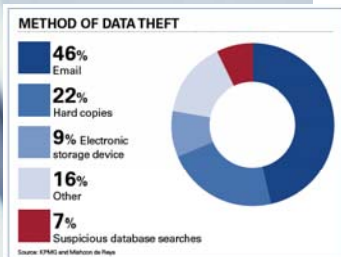
In today's fast moving business world, technology platforms and systems play a critical role in the achievement of business objectives. It is essential that the risks are identified and assessed to ensure they are being effectively managed.

Therefore, IT security is becoming more and more a concern for members of management, as their responsibility becomes directly involved.

To the extent of IT security, a certain number of questions should be raised, such as:

- Has data security been identified as a significant or strategic risk in the company's ongoing risk assessment process?
- Has the company assigned executive responsibility for data security and protection?
- Has the company taken effective measures to protect against unauthorized data or security disclosure?
- Does the company have an effective program for monitoring controls or has it recently evaluated its specific risks and regulatory requirements regarding all data that is stored, processed or used by the company?
- What are the ongoing metrics and key performance indicators to be used to monitor compliance with established policies and controls?
- Has the company established an effective program for responding to a potential disclosure or data-loss event?

A profound review on IT security and implemented controls will help to identify potential for improvement.



## IT security

- User Access Management - Segregation of Duties (SoD)
- System landscapes and Interfaces
- Banking systems (parameterization, logging, Security, SoD)
- Processes and procedures (also third party involvement)
- Data confidentiality, integrity, availability
- Network, hardware infrastructure, physical security
- Applications, operation systems, firewalls

## IT controls/IT control framework

- Using recognized standards (COBIT, ITIL, ISO 27001)
- Documentation of processes and controls
- Manual versus automatic controls
- Evaluation of design and implementation, test on operating effectiveness

## External/Internal security testing

- Penetration (black box, white box), Web-App
- Intrusion Detection

## Risk/Impact analysis

- Regulatory and compliance
- Operational, Financial, Reputation

## Change Management

- Risk awareness training
- Adaption of processes and procedures

## Monitoring of IT systems

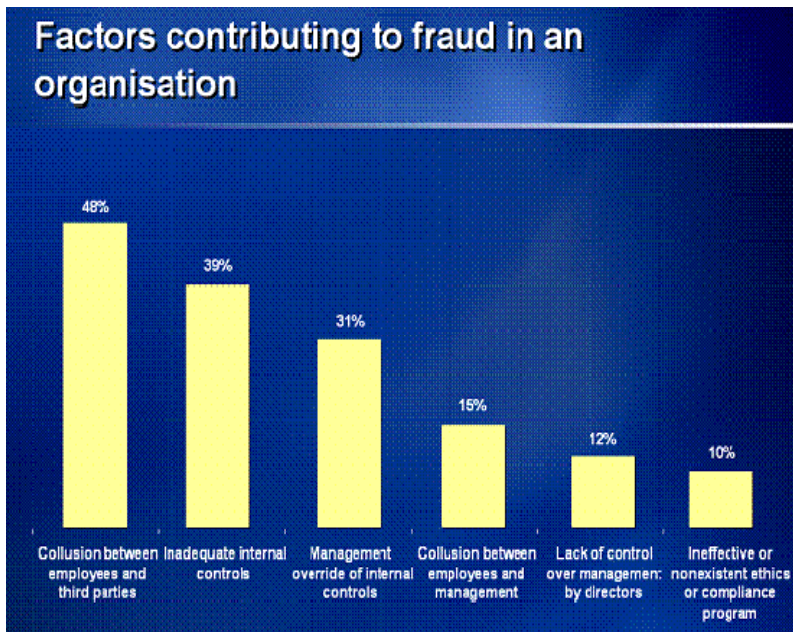
- Management Information System (MIS)
- Key Performance Indicators (KPI)

## Preventive and Crisis management

# The Forensic Perspective

**Fraud** is a broad legal concept that generally refers to an intentional act committed to secure an unfair or unlawful gain

**Misconduct** is a broad concept, referring to violations of laws, regulations, internal policies, and market expectations for ethical business conduct.



People are not born fraudster but become so. This does not mean that each employee is a potential fraudster, but it rather leads to the question : "Why do people commit fraud?"

There are three important factors concerned with committing fraud: Opportunity, Incentive/Pressure and Rationalization (ref. "The Fraud Triangle")

- **Opportunity** occurs generally through weaknesses in the internal controls and contributes to create an atmosphere where fraudsters believe they are likely to be successful and undetected.
- **Incentive/Pressure** might result from a fraudster's excessive life style, from pressure to meet targets, from the financial remuneration earned by the individual, etc.
- **Rationalization** is the self justification found by the fraudster for his actions (ex: they do not pay me enough, who cares?, rules are made to be broken)

# The Forensic Perspective

**Our approach** is based on a specific fraud risk management methodology that assist clients in their efforts to prevent, detect and respond appropriately to fraud and misconduct risks, through the design, implementation and evaluation of antifraud programs and controls. This approach is tailored made to the client and its activities.



## **Prevention**

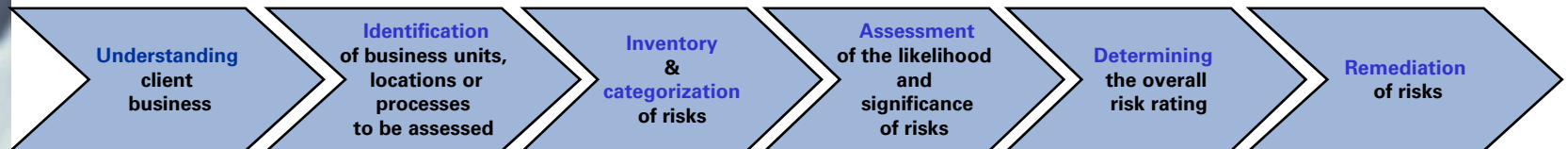
A comprehensive fraud and misconduct risk assessment helps management understand their business unique risks, identify gaps or weaknesses in their controls and develop a plan for targeting the right resources and controls

## **Detection**

Detective controls are designed to uncover fraud and misconduct when it occurs

## **Response**

Responsive controls are designated to take corrective action and remedy the harm caused by fraud and misconduct



# The Processes & People Perspective

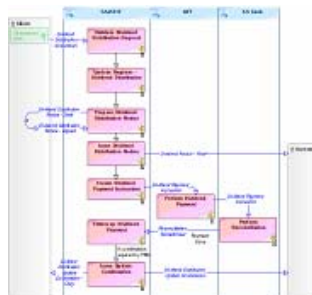
## Processes

Although security cannot constitute an obstacle to the operational fluidity of activities, it is nonetheless essential to consider, in every step of every major process, the associated risks.

To that extent, a certain number of questions should be raised, such as:

- How many people, within a given process, should be granted access to sensitive information?
- What data do I need to handle this specific operation?
- Is there too many data available for this specific process?
- What are the processes in place to deter confidentiality breach?
- How do private bankers manage their customers' data?
- Etc.

A review of the existing processes makes it possible to question the current modus operandi, identify and assess the risks and take appropriate mitigation measures.



## People

Obviously, the management of confidential data very much relies on the resources *per se* of banking institutions. To that extent, it is important for banks to be able to assess the capability of their own resources to manage and maintain a high level of professionalism and loyalty.

In addition, due to, among other, the large heterogeneity of resources working in banks, ensuring that all employees adopt a similar and consistent approach towards banking secrecy and data management, is also another crucial issue.

In a context where most banks organize training and awareness sessions to ensure that their resources are very much aware of the importance of banking secrecy, there seems to be less and less leniency towards resources not complying with rules and regulations.

As depicted above, people-related issues are key and should undoubtedly be carefully analyzed to ensure that all the necessary actions have been taken beforehand.

# How can KPMG assist you?

## How does it work ?

In order to assess the current situation in your Organization and benchmark it with state-of-the-art practices, we propose a pragmatic analysis during which we will interview key resources within your Organization (individually or in group):

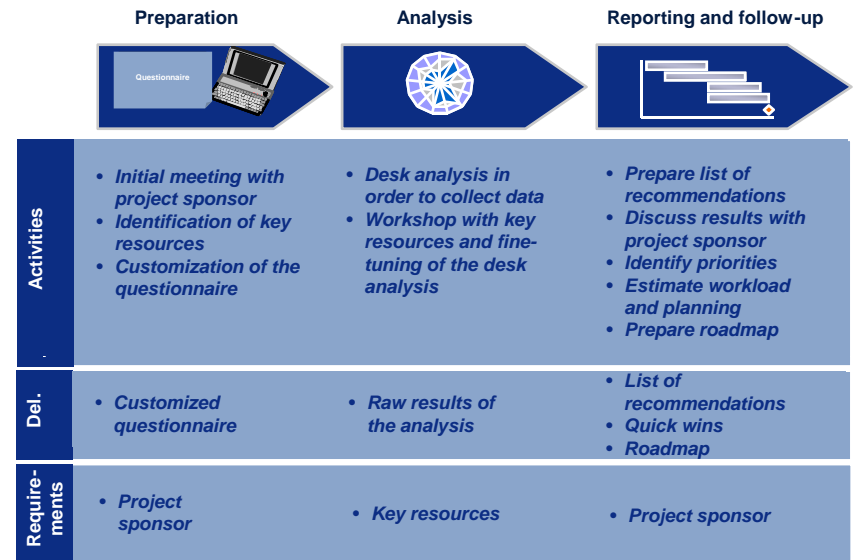
- Management
- Information Technology
- Organization
- Human Resources
- Compliance/Legal
- Internal Audit
- Communication

The analysis consists of easy to follow steps. The summary on the right provides an outline of which activities will be performed and which products they deliver.

## Results

As a product of this analysis, you will receive two main deliverables :

- A list of recommendations with a high-level project plan
- A list of quick wins that could be easily implemented in a short-term perspective



## Team

- KPMG has put together a team of experienced professionals combining a comprehensive set of competences and skills.
- KPMG professionals are certified in their area of expertise, e.g. CISA, CISSP, CFE, Six Sigma

# The German Tax Perspective

## **Factual situation**

In the recent past the renowned banking secrecy of Luxembourg has been lifted in many areas due to international pressure. Whereas Luxembourg did maintain its banking secrecy for non-residents by introducing a withholding tax on interest paid to the latter, it was not able to elude cooperation with German tax authorities with respect to the exchange of information regarding German citizens especially in cases of a suspicion of tax evasion. Premise for such cooperation is a prima facie evidence of tax fraud which is now amply supplied by banking client data that has been breached on stolen CD and is currently being sold to the German tax authorities.

In case that Luxembourg income has not or not been properly filed in the past the bank customer might be accused of tax evasion. Besides a criminal punishment the bank customer will have to pay the evaded taxes plus interest thereon.

## **Issues for the individual**

In such a case what must be done if ...

- there is a high risk of detection (due to e.g. data theft) regarding non declared assets in Luxembourg?
- a bank customer wishes to declare its hidden assets in Luxembourg based on personal motives (e.g. upcoming succession)?

To be exempt from criminal punishment the bank customer will need to report himself (self-denunciation) before the discovery of

the crime by the tax authority and will have to

- amend all his tax returns by declaring his income completely and free of errors (this can go back up to 13 years),
- inform the tax authorities about the amount of non-declared inheritance or gift respectively;
- pay the evaded taxes (including interests) in due time.

## **Issues for the bank**

The banks are advised to assist and support their customer in this clarification process as the latter might not have all the relevant information and data to properly assess and / or calculate his taxable income. With respect to the detailed German tax provisions regarding the qualification and taxation of capital income which, furthermore, did significantly change in the past years, a throughout understanding of the German taxation rules of the past 13 years is required.

## **Issues for investment funds**

Many investment funds have not complied with the tax provisions regarding the fiscal transparency of the investment fund in Germany. German unit fund holders did not requested such treatment as they did not declare the respective income from the funds in Germany. Hence, the unfavorable lump-sum taxation for non-transparent funds did effectively not apply. In order to reduce the amount of evaded taxes it is recommended that the investment fund concerned establish retroactively the fund's tax transparency (up to 13 years).

www.kpmg.lu

Michael Hofmann  
Partner  
Tel:+352 22 51 51 7925  
Mob: +352 621 87 7925  
michael.hofmann@kpmg.lu



Jean Pascal Nepper  
Director  
Tel:+352 22 51 51 7973  
Mob: +352 621 87 7973  
jean-pascal.nepper@kpmg.lu



Thomas Thiel  
Senior Manager  
Tel:+352 22 51 51 7944  
Mob: +352 621 87 7944  
thomas.thiel@kpmg.lu



Sandrine Periot  
Senior Manager  
Tel:+352 22 51 51 7220  
Mob: +352 621 87 7220  
sandrine.periot@kpmg.lu



The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2010 KPMG Advisory S.à r.l., a Luxembourg private limited company, is an affiliate of KPMG Europe LLP and a member firm of the KPMG network of independent member firms affiliated with KPMG International cooperative ("KPMG International"), a Swiss entity. All rights reserved. KPMG and the KPMG logo are registered trademarks of KPMG International. Printed in Luxembourg.