



IT Advisory Services

## Mobile Data in a larger perspective

ADVISORY

AUDIT ■ TAX ■ ADVISORY

## Contents


- **Various frameworks and approaches**
- **Risk Management**
- **Baselining**
- **Information Governance - Information LifeCycle Management**
- **Data Classification**
- **Mobile data**



# Enterprise Risk Management frameworks

Organizations should select a framework or confirm the existence of a framework that is appropriate and robust.

There are a number of frameworks to choose from:

<p>Committee of sponsoring organizations ("COSO") ERM</p> 	<p>Turnbull / Flint UK</p>
<p>Her Majesty's ("HM") Treasury UK</p>	<p>Australia / New Zealand ("AS/NZ") Risk Management standard 4360</p>

KPMG Risk Management Framework

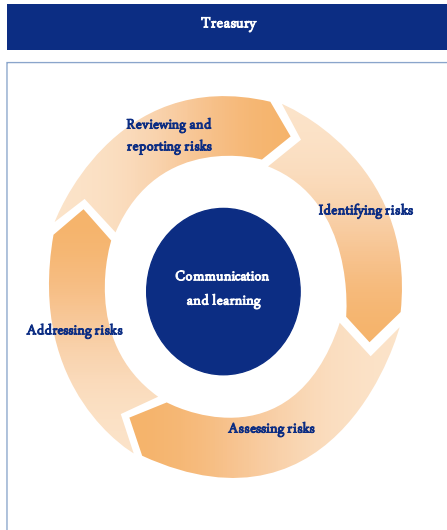
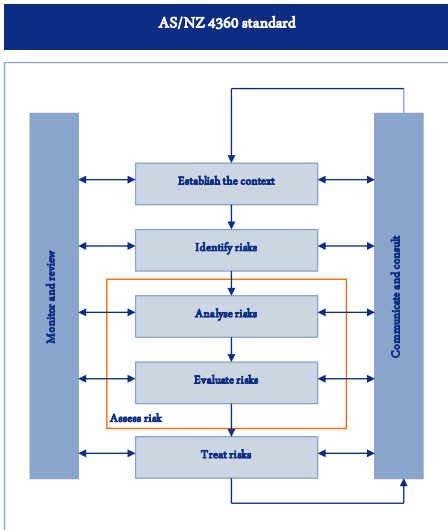


The content of the framework will provide a clear structure for your risk management activity.



© 2009 KPMG Advisory, a civil limited cooperative company (known by the Dutch initials BCVBA; known by the French initials SCRL civile) and a member firm of the KPMG network of independent member firms affiliated with KPMG International, a Swiss cooperative. All rights reserved.

# Frameworks

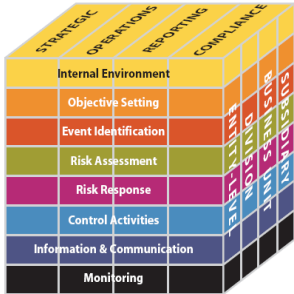


© 2009 KPMG Advisory, a civil limited cooperative company (known by the Dutch initials BCVBA; known by the French initials SCRL civile) and a member firm of the KPMG network of independent member firms affiliated with KPMG International, a Swiss cooperative. All rights reserved.

# Frameworks (continued)

## COSO ERM

- Internal environment**
  - Philosophy regarding risk management
  - Establish risk culture
  - Affect on risk culture
- Monitoring**
  - Ongoing monitoring activities
  - Separate evaluations
  - Combination of two
- Information and Communication**
  - Identification, capture and communication of pertinent information throughout the organization
- Control activities**
  - Policies and procedures
  - All levels and functions



- Risk response**
  - Identifies and evaluates responses to risk
  - Evaluates options in relation to risk appetite, cost vs. benefit, effect on likelihood / impact
  - Selects and executes response

- Objective setting**
  - Consideration of risk strategy in objective setting
  - Forms the risk appetite of the entity
  - Risk tolerance aligned with risk appetite
- Event identification**
  - Differentiates risks and opportunities
  - Opportunities channelled into strategy setting
  - Addresses how internal and external factors combine and interact to influence the risk profile
- Risk assessment**
  - An events' impact on objectives
  - Quantitative and qualitative methodologies
  - Time horizons
  - Inherent and residual

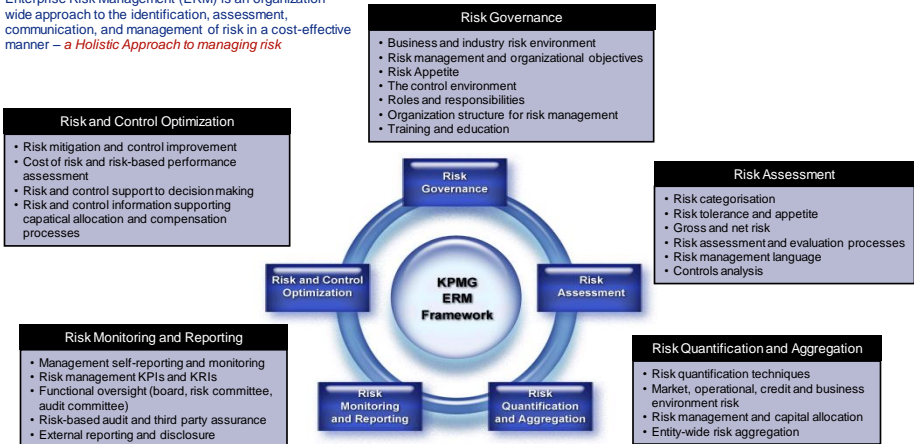


© 2009 KPMG Advisory, a civil limited cooperative company (known by the Dutch initials BCVBA; known by the French initials SCRL civile) and a member firm of the KPMG network of independent member firms affiliated with KPMG International, a Swiss cooperative. All rights reserved.

# Frameworks (continued)

## KPMG's View on ERM:

Enterprise Risk Management (ERM) is an organization-wide approach to the identification, assessment, communication, and management of risk in a cost-effective manner – a *Holistic Approach to managing risk*

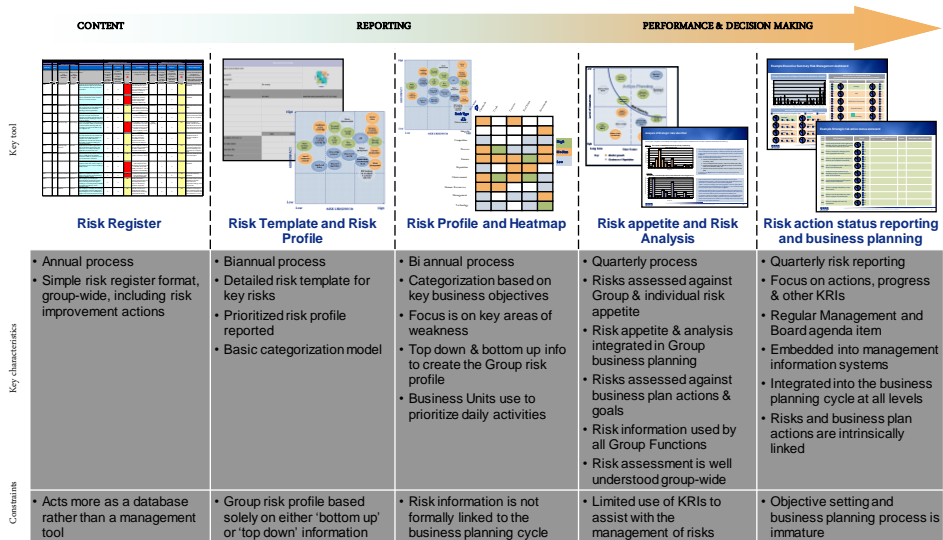


ERM is a dynamic process which is focused on *protecting* an organization's *value proposition*



© 2009 KPMG Advisory, a civil limited cooperative company (known by the Dutch initials BCVBA; known by the French initials SCRL civile) and a member firm of the KPMG network of independent member firms affiliated with KPMG International, a Swiss cooperative. All rights reserved.

# Determining the risk profile



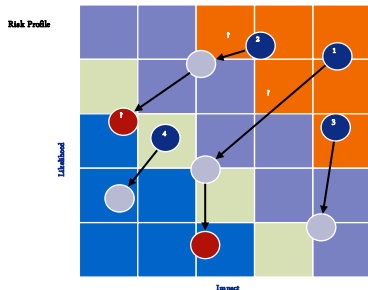
© 2009 KPMG Advisory, a civil limited cooperative company (known by the Dutch initials BCVBA; known by the French initials SCRL civile) and a member firm of the KPMG network of independent member firms affiliated with KPMG International, a Swiss cooperative. All rights reserved.

7

# Reporting risks

There are a number of simple tools that present risk information in such a way as to make it easy to review and challenge.

## 1. What are our key risks?



## 2. What does this tell you?

- Key risks and their significance vs. appetite
- Concentrations of risk
- Control effectiveness and reliance
- Gaps in perceived risk across business
- Opportunities for control rationalization
- Controls that reduce likelihood and those that reduce impact



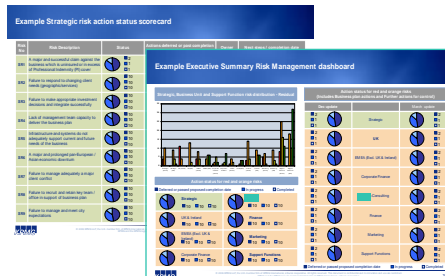
© 2009 KPMG Advisory, a civil limited cooperative company (known by the Dutch initials BCVBA; known by the French initials SCRL civile) and a member firm of the KPMG network of independent member firms affiliated with KPMG International, a Swiss cooperative. All rights reserved.

8

## 3. What else is important?

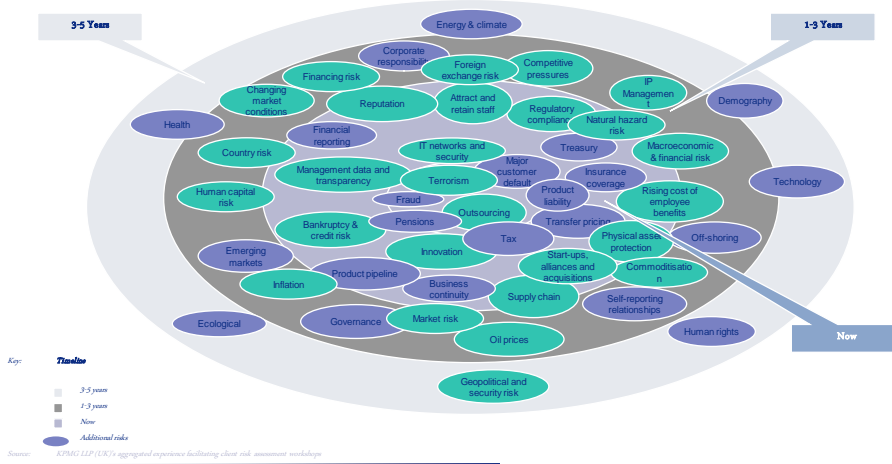
- Movement over time
- Risk trends
- Where assurance comes from
- Context commentary from management
- Improvement areas and associated actions
- Action and accountability update

## 4. What should be reported and when?



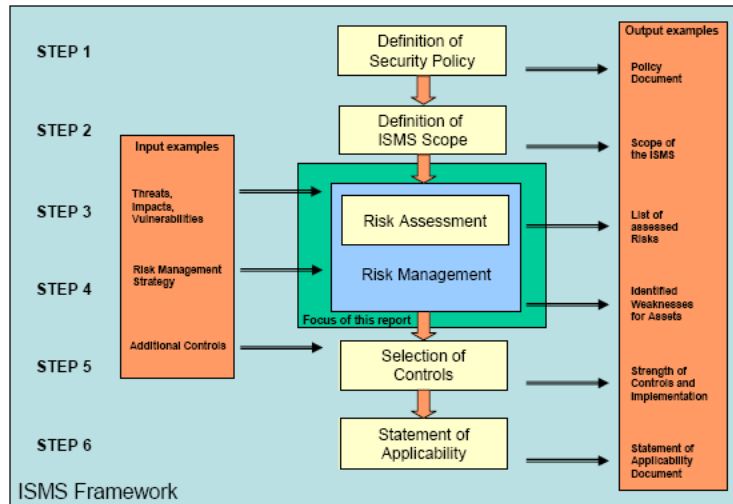
# Our experience of a typical risk profile confirms there are broader risks to think about

When you look at a typical risk profile now compared to three years ago there are many more potential risks. To make sense of this, you need to think about the time horizon to know where to focus.



© 2009 KPMG Advisory, a civil limited cooperative company (known by the Dutch initials BCVBA; known by the French initials SCRL civile) and a member firm of the KPMG network of independent member firms affiliated with KPMG International, a Swiss cooperative. All rights reserved. 9

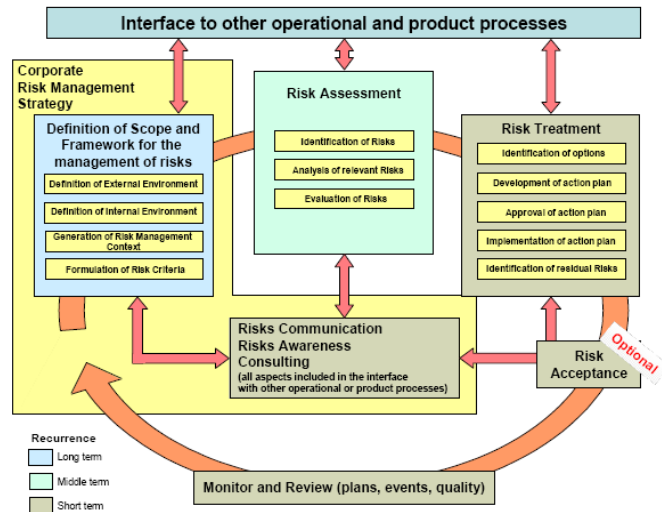
# Risk Management within an Information Security Management System



Source: ENISA publication: Risk Management: Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools, June 2006

© 2009 KPMG Advisory, a civil limited cooperative company (known by the Dutch initials BCVBA; known by the French initials SCRL civile) and a member firm of the KPMG network of independent member firms affiliated with KPMG International, a Swiss cooperative. All rights reserved. 10

# Risk Management within an Information Security Management System

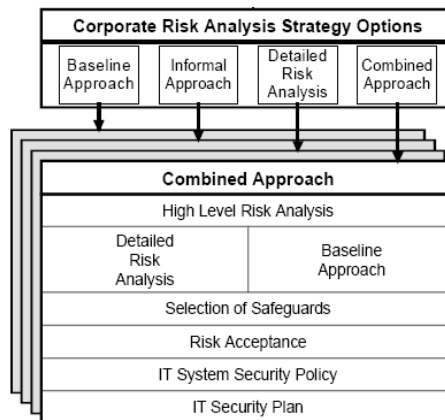


Source: ENISA publication: Risk Management: Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools, June 2006



© 2009 KPMG Advisory, a civil limited cooperative company (known by the Dutch initials BCVBA; known by the French initials SCRL civile) and a member firm of the KPMG network of independent member firms affiliated with KPMG International, a Swiss cooperative. All rights reserved.

# Techniques for Management of IT Security



Source: ISO TR 13335-3, Information Technology – Guidelines for the management of IT Security – Part 3: Techniques for the management of IT Security



© 2009 KPMG Advisory, a civil limited cooperative company (known by the Dutch initials BCVBA; known by the French initials SCRL civile) and a member firm of the KPMG network of independent member firms affiliated with KPMG International, a Swiss cooperative. All rights reserved.

# Information Governance – Information LifeCycle Management

*Information Governance is KPMG's management framework that helps clients protect information based on its business value and associated risks.*

KPMG's Information Governance services assist organizations with designing personnel, process, technology, and controls that address compliance requirements, while also protecting the most important information assets

KPMG's approach encompasses the complete governance lifecycle, helping to enable clients to choose the appropriate services to achieve their specific business needs.



© 2009 KPMG Advisory, a civil limited cooperative company (known by the Dutch initials BCVBA; known by the French initials SCRL civile) and a member firm of the KPMG network of independent member firms affiliated with KPMG International, a Swiss cooperative. All rights reserved.

# Information Governance – Information LifeCycle Management

**Information LifeCycle Management (ILM)**  
The core of our approach focuses on ILM which comprises the policies, processes, practices, and tools used to align the business value of information with the most appropriate and cost effective IT infrastructure -- from the time information is conceived through its final disposition.

**Privacy**  
The handling and protection of personal identifiable information (PII) that individuals provide in the course of everyday transactions, electronically or otherwise.

**IT Security**  
The process of protecting data from unauthorized access, use, disclosure, destruction, modification, or disruption.

**Third-Party Management**  
The process of managing external entities that may process or store information owned or originated by an organization.

**eRecords Management**  
The planning, controlling, directing, organizing, training, promoting, and other managerial activities related to the creation, maintenance and use, and disposition of electronic records.

**Data Flow Analytics**  
The process of classifying and managing the flow of information assets within an organization.

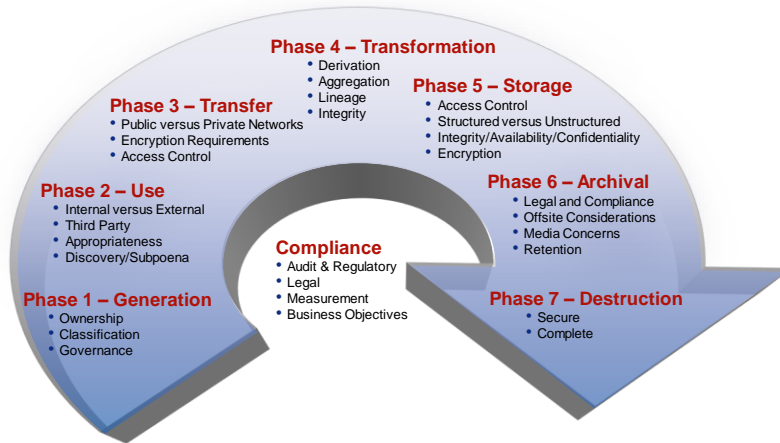
**Data Classification**  
The process of dividing data sources (documents, applications, databases, etc.) into groupings to which defined level of controls, protection and policies can be applied to support business objectives.



© 2009 KPMG Advisory, a civil limited cooperative company (known by the Dutch initials BCVBA; known by the French initials SCRL civile) and a member firm of the KPMG network of independent member firms affiliated with KPMG International, a Swiss cooperative. All rights reserved.

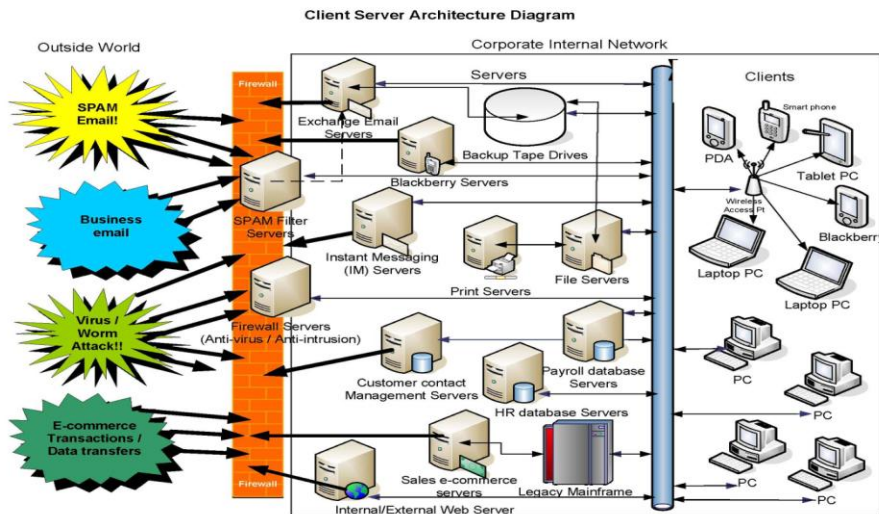
# Information LifeCycle Management

KPMG's approach also aims to gain an understanding of the risks associated with your information across its lifecycle. Key considerations are as follows:



© 2009 KPMG Advisory, a civil limited cooperative company (known by the Dutch initials BCVBA; known by the French initials SCRL civile) and a member firm of the KPMG network of independent member firms affiliated with KPMG International, a Swiss cooperative. All rights reserved.

# Where is my information ?



Microsoft submission to Federal Rules Committee



© 2009 KPMG Advisory, a civil limited cooperative company (known by the Dutch initials BCVBA; known by the French initials SCRL civile) and a member firm of the KPMG network of independent member firms affiliated with KPMG International, a Swiss cooperative. All rights reserved.

## What about here?



© 2009 KPMG Advisory, a civil limited cooperative company (known by the Dutch initials BCVBA; known by the French initials SCRL civile) and a member firm of the KPMG network of independent member firms affiliated with KPMG International, a Swiss cooperative. All rights reserved.

18

## Potential Data Privacy Breach Costs

### Measurable Costs \*

Average costs to address a breach:	Direct incremental cost:	Lost productivity costs:	Customer opportunity costs:
<ul style="list-style-type: none"> <li>• \$197 per compromised record</li> <li>• \$6.3 million per breach, ranging from \$226,000 to \$22 million</li> </ul>	<ul style="list-style-type: none"> <li>• \$54 per lost record</li> <li>• Unbudgeted, out-of-pocket spending. Includes free or discounted services offered; notification letters, phone calls, and emails; legal, audit and accounting fees; call center expenses; public and investor relations; and other costs.</li> </ul>	<ul style="list-style-type: none"> <li>• Averaged \$30 per lost record for lost employee or contractor time and productivity diverted from other tasks</li> </ul>	<ul style="list-style-type: none"> <li>• Averaged \$128 per lost record, covering turnover of existing customers and increased difficulty in acquiring new customers</li> </ul>

\*Ponemon Institute, LLC, November 2007, "2007 Annual Study: Cost of a Data Breach" -- Examined the costs incurred by companies after experiencing an actual data breach. Results were not hypothetical responses; they represent cost estimates for activities resulting from actual data loss incidents.

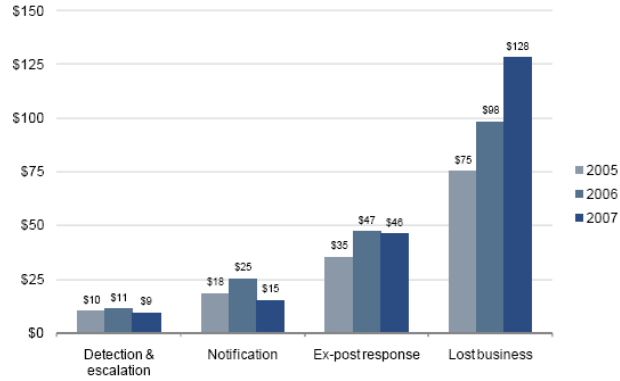


© 2009 KPMG Advisory, a civil limited cooperative company (known by the Dutch initials BCVBA; known by the French initials SCRL civile) and a member firm of the KPMG network of independent member firms affiliated with KPMG International, a Swiss cooperative. All rights reserved.

19

# What could a Data Privacy Breach Cost Me?

Data breach costs by center per record compromised, 2005–2007 \*



\*Ponemon Institute LLC, November 2007, "2007 Annual Study: Cost of a Data Breach" – Examined the costs incurred by companies after experiencing an actual data breach. Results were not hypothetical responses; they represent cost estimates for activities resulting from actual data loss incidents.



© 2009 KPMG Advisory, a civil limited cooperative company (known by the Dutch initials BCVBA; known by the French initials SCRL civile) and a member firm of the KPMG network of independent member firms affiliated with KPMG International, a Swiss cooperative. All rights reserved.

**KPMG**

FINANCIAL ADVISORY SERVICES

## Data Loss Barometer - Survey

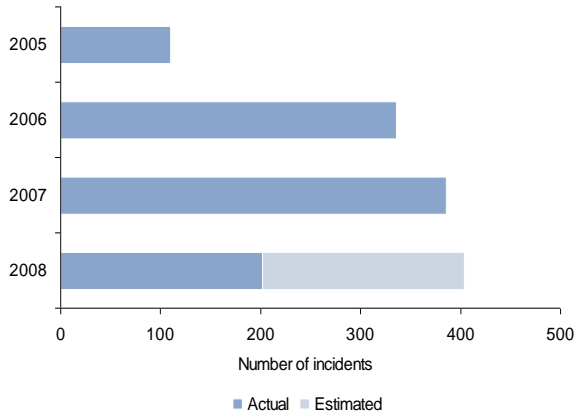
September 2008

ADVISORY

AUDIT • TAX • ADVISORY

# Data loss – The scale of the problem

## Data loss incidents vs. year



- 1034 data loss incidents since January 2005
- Increasing technology reliance contributes to an increasing number of incidents

Source: KPMG LLP (UK)

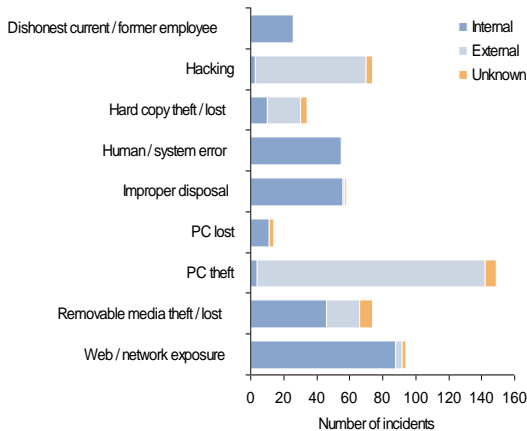


© 2009 KPMG Advisory, a civil limited cooperative company (known by the Dutch initials BCVBA; known by the French initials SCRL civile) and a member firm of the KPMG network of independent member firms affiliated with KPMG International, a Swiss cooperative. All rights reserved.

22

# Data loss Incidents

## Number of incidents vs. type of breach



- 589 incidents since January 2007
- 25% involve PC theft
- 16% web/network exposure
- 13% hacking

Source: KPMG LLP (UK)

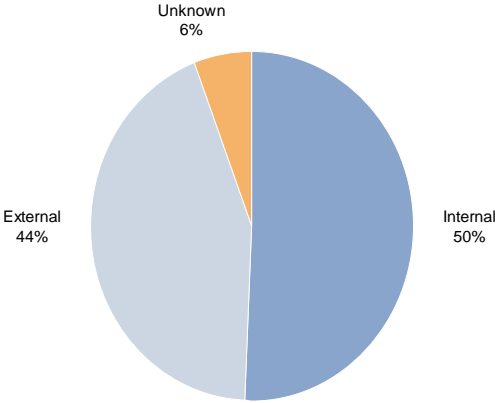


© 2009 KPMG Advisory, a civil limited cooperative company (known by the Dutch initials BCVBA; known by the French initials SCRL civile) and a member firm of the KPMG network of independent member firms affiliated with KPMG International, a Swiss cooperative. All rights reserved.

23

# Data loss source

## Security breach source



- External breaches are more difficult to predict and control
- Internal breaches are more common

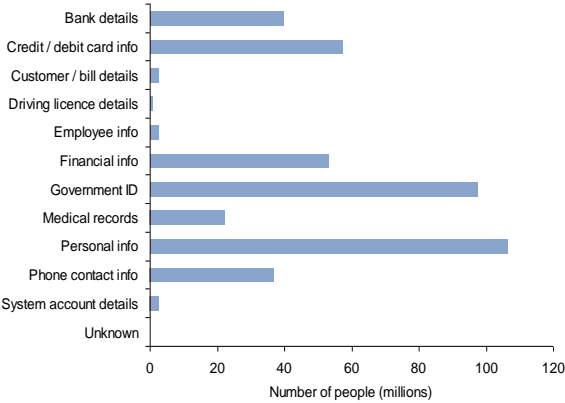
Source: KPMG LLP (UK)



© 2009 KPMG Advisory, a civil limited cooperative company (known by the Dutch initials BCVBA; known by the French initials SCRL civile) and a member firm of the KPMG network of independent member firms affiliated with KPMG International, a Swiss cooperative. All rights reserved.

# Types of data loss

## People affected vs. data type



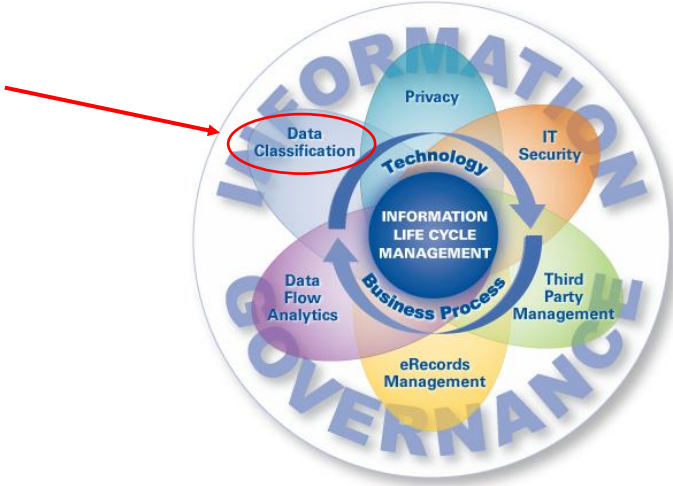
- 77m people had personal data revealed
- 139m disclosures relate to financial information
- Preventative rather than reactive measures are key to data protection

Source: KPMG LLP (UK)



© 2009 KPMG Advisory, a civil limited cooperative company (known by the Dutch initials BCVBA; known by the French initials SCRL civile) and a member firm of the KPMG network of independent member firms affiliated with KPMG International, a Swiss cooperative. All rights reserved.

# Information LifeCycle Management – Data Classification



© 2009 KPMG Advisory, a civil limited cooperative company (known by the Dutch initials BCVBA; known by the French initials SCRL civile) and a member firm of the KPMG network of independent member firms affiliated with KPMG International, a Swiss cooperative. All rights reserved.

## Why classify data?

Increasingly, organizations are leveraging data classification programs as a foundation for (a) identifying their most valuable and risky information assets and (b) re-allocating resources to address its most valuable and risky information assets.

Specifically, a data classification program can assist with:

- Client & Customer**

}

  - Meet client expectations and requests
  - Assist with marketing initiatives
  - Improve and instill confidence of customers, clients, employees, and business partners
  
- Compliance & Financial**

}

  - Meet regulatory and compliance obligations
  - Achieve and sustain the increasing number of external partner and audit requirements
  - Improve information management and protection
  - Re-allocate resources to align financial spend to the information assets that are most valuable or risky
  - Improve business intelligence by further understanding how the organization utilizes its information assets



© 2009 KPMG Advisory, a civil limited cooperative company (known by the Dutch initials BCVBA; known by the French initials SCRL civile) and a member firm of the KPMG network of independent member firms affiliated with KPMG International, a Swiss cooperative. All rights reserved.

# What is Data Classification?

## Data Classification Defined

- Framework by which value is placed on information, so it can be managed with appropriate levels of sensitivity and protection;
- Used as a tool to determine how much effort, money, and resources are allocated to protect data and control access and use; and
- Program to be used by all employees and trusted third parties who handle information on behalf of the organization.



# Sample data classification

Sample data classifications include:

- **PUBLIC**: Information used to promote, share, or openly communicate with anyone;
- **INTERNAL USE ONLY**: information shared internally across business units, teams, and partners;
- **CONFIDENTIAL**: information distributed on a “need to know” basis only; and
- **SECRET**: confidential information that is purposefully designated or identified as restricted due to its significant value and/or risk to the organization

Sensitive



**Remember...**  
Information assets may start out as Confidential, but then end up as Public.  
Information can change its classification over time!!



# Four classifications provide a practical way to manage the costs associated with protecting information assets

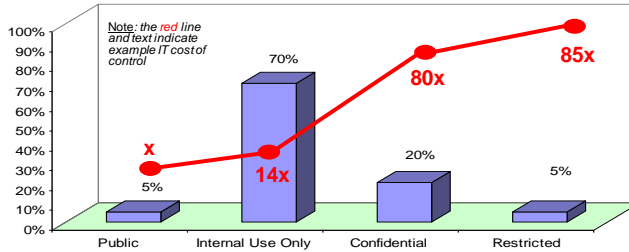
Classification Schema

Public    Internal Use Only    Confidential    Secret

Ex. Information Asset

Charitable Announcement    Intranet    Customer Application Password File

Information Asset Distribution and IT Security Cost of Control (factors are an example)



Representative Controls

- No controls
- ✓ Strong password
- ✓ Inactivity Timeout
- ✓ Current Antivirus
- ✓ "Confidential" Label
- ✓ Transfer Encryption
- ✓ Confirmation of receipt
- ✓ Printed reports locked away
- ✓ Storage Encryption
- ✓ Transfer encryption
- ✓ Host IDS
- ✓ Audit Trail
- ✓ Character Masking



© 2009 KPMG Advisory, a civil limited cooperative company (known by the Dutch initials BCVBA; known by the French initials SCRL, civile) and a member firm of the KPMG network of independent member firms affiliated with KPMG International, a Swiss cooperative. All rights reserved.

32

# Sample Data Classification Controls Matrix

Actions	Accessing	Delegating	Storing	Sending	Bulk Distrib.	Backing-up	Copying	Retaining	Disposing
<b>Secret</b>	Granted to select individuals only. System specific authorization; network authentication at a minimum. Dual factor authentication should be considered.	Not permitted	Encrypted	Encrypted	Not permitted	Encrypted.	Should be encrypted on removable media.	Granular and non-automatic retention required.	Physically destroy all disposable removable media. Secure wipe all copies from hard disks, and from permanent removable media etc.
<b>Confidential</b>	Granted to discrete user groups only. System specific authorization; network authentication at a minimum.	User controlled delegation is permitted; delegation may not be automated. No external delegation. Granularity of actions delegated should be considered.	Clear text is permissible. Encryption should be considered where appropriate.	External Encryption required for external transmission; clear text permitted with client consent.  Internal Clear text permitted.	Encrypted	Encryption should be considered where appropriate	Should be encrypted on removable media.	Granular and non-automatic retention required.	Physically destroy all disposable removable media. Secure wipe all copies from hard disks, and from permanent removable media.



© 2009 KPMG Advisory, a civil limited cooperative company (known by the Dutch initials BCVBA; known by the French initials SCRL, civile) and a member firm of the KPMG network of independent member firms affiliated with KPMG International, a Swiss cooperative. All rights reserved.

33

## Sample Data Classification Controls Matrix

Actions	Accessing	Delegating	Storing	Sending	Bulk Distrib.	Backing-up	Copying	Retaining	Disposing*
<b>Internal Use Only</b>	Granted to internal XXX staff, recruitment agencies, and business partners. Network authentication is required.	NA	Clear text is permissible.	Clear text permitted.	Clear text permitted. Encryption should be considered where appropriate.	Clear text is permissible	May be copied but custody should be limited to XXX	Automatic retention.	Physically destroy all disposable removable media. Delete all copies from hard disks, and from permanent removable media.
<b>Public</b>	General Public No requirement for authentication.	NA	Clear text	Clear text	Clear text	Clear text	No restrictions.	Automatic retention.	Delete files from hard disks.



© 2009 KPMG Advisory, a civil limited cooperative company (known by the Dutch initials BCVBA; known by the French initials SCRL civile) and a member firm of the KPMG network of independent member firms affiliated with KPMG International, a Swiss cooperative. All rights reserved.

34

## Case: mobile data on PDA

Which level of data can be used on the PDA ?

Confidential => Min. required controls:

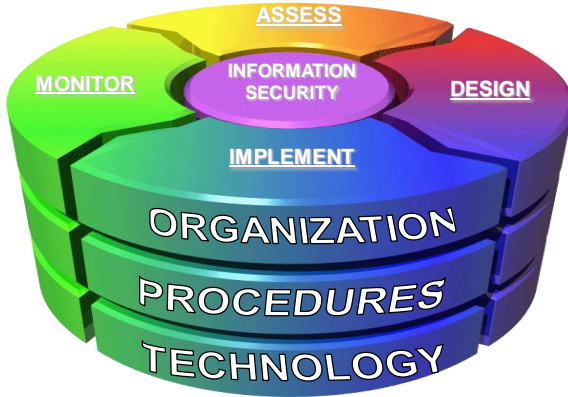
- Accessing: password-based authentication
- Storage: encrypted
  - Internal file system
  - External file system (SD card)
- Transmission: encrypted
- Copying: encrypted on removable media
- Disposing: secure wipe



© 2009 KPMG Advisory, a civil limited cooperative company (known by the Dutch initials BCVBA; known by the French initials SCRL civile) and a member firm of the KPMG network of independent member firms affiliated with KPMG International, a Swiss cooperative. All rights reserved.

35

# Control domains



**Summary**

The document contains the security guidelines of KPMG in Belgium. It is intended for all employees of KPMG in Belgium and is subject to the internal security policy of KPMG in Belgium. The document is subject to the internal security policy of KPMG in Belgium.

**Approved by:**

- Director of KPMG in Belgium
- Director of KPMG in Belgium
- Director of KPMG in Belgium
- Director of KPMG in Belgium

**Approved on:**

15/11/2008

**Approved by:**

Director of KPMG in Belgium



**Summary**

The document contains the guidelines for the use of BlackBerry devices. It is intended for all employees of KPMG in Belgium and is subject to the internal security policy of KPMG in Belgium. The document is subject to the internal security policy of KPMG in Belgium.

**Approved by:**

- Director of KPMG in Belgium
- Director of KPMG in Belgium
- Director of KPMG in Belgium
- Director of KPMG in Belgium

**Approved on:**

15/11/2008

**Approved by:**

Director of KPMG in Belgium



© 2009 KPMG Advisory, a civil limited cooperative company (known by the Dutch initials BCVBA; known by the French initials SCRL civile) and a member firm of the KPMG network of independent member firms affiliated with KPMG International, a Swiss cooperative. All rights reserved.

# Questions ?



The special bulletin for recipients of KPMG's Data Loss Barometer provides an update on data losses during 2008 and predictions for 2009.

In 2008, global incidents of data loss increased in number. With widely reported media stories of inadvertent loss or theft, it is an issue that has become firmly embedded in the public conscience. For the organizations affected, and the millions of innocent people whose data is exposed, the impact of large-scale data loss can be brutal.

As the global economic downturn deepens, we expect data loss to continue to increase in 2009. Organizations across the public and private sectors, with budgets already squeezed, will continue to be vulnerable to loss of sensitive data. Sophisticated organized criminals will seek to exploit these weaknesses for financial gain. It looks like the credit crunch will also lead to a "data crunch".

From last year...	To remain...
<ul style="list-style-type: none"> <li>Decreased for 2008</li> <li>A record 677 data loss incidents reported in 2008, an average of 1.8 incidents per organization</li> <li>412 million people were affected in the 2008 incidents</li> <li>More than the total of the year covered</li> <li>A 50 per cent year on year increase in the number of people affected by data loss</li> </ul>	<ul style="list-style-type: none"> <li>Increased for 2009</li> <li>If the trend since September 2008 continues, over 100 million people will be affected in 2009</li> <li>We expect the number of reported incidents to increase by about 10 percent</li> <li>That may translate into an expected 100 million people affected</li> </ul>

**2008 Data Loss Barometer highlights**

- an estimated 677 global data loss incidents reported in 2008, an average of 1.8 incidents per organization
- 412 million people were affected in the 2008 incidents
- More than the total of the year covered
- A 50 per cent year on year increase in the number of people affected by data loss

**2009 Data Loss Barometer highlights**

- an estimated 100 million people will be affected in 2009
- We expect the number of reported incidents to increase by about 10 percent
- That may translate into an expected 100 million people affected

**2007 Data Loss Barometer highlights**

- an estimated 350 million people were affected in 2007
- We expect the number of reported incidents to increase by about 10 percent
- That may translate into an expected 100 million people affected

**2008 Data Loss Barometer highlights**

- an estimated 412 million people were affected in 2008
- We expect the number of reported incidents to increase by about 10 percent
- That may translate into an expected 100 million people affected

**2009 Data Loss Barometer highlights**

- an estimated 100 million people will be affected in 2009
- We expect the number of reported incidents to increase by about 10 percent
- That may translate into an expected 100 million people affected



© 2009 KPMG Advisory, a civil limited cooperative company (known by the Dutch initials BCVBA; known by the French initials SCRL civile) and a member firm of the KPMG network of independent member firms affiliated with KPMG International, a Swiss cooperative. All rights reserved.

Want to know more ? Contact us

**Dirk De Maeyer**  
 Manager, IT Advisory – Information Protection and Business Resilience  
 Data Protection Officer  
 National IT Security Officer

+32 2 708 4707  
[ddemaeyer@kpmg.com](mailto:ddemaeyer@kpmg.com)

