


18275-F1BOS

**You can outsource liability  
you can't outsource responsibility and accountability!**



© 2007 KPMG LLP, a U.S. limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International, a Swiss cooperative. All rights reserved. Printed in the U.S.A.

1



## Introduction



18275-F1BOS

## Sourcing defined

<b>Outsourcing</b>	A long-term, results-oriented relationship with an external service provider for activities traditionally performed within the company
<b>Off-shoring</b>	Allocation of IT enabled processes to be managed by an internal/external service provider at a remote location, i.e. at centres in countries outside the originating location
<b>Near-shoring</b>	Offshore activities within nearby territory, and accessible by short travel or telephone in the same or neighbouring time zone
<b>Business process outsourcing (BPO)</b>	The delegation of one or more business processes to an external service provider who in turn, owns, administers and manages the selected process / processes, based upon defined and measurable performance metrics
<b>Shared services, captive</b>	The consolidation of common functions, systems, processes and personnel across several business units into an internal service bureau, managed as an independent organisation
<b>In-sourcing, back-sourcing</b>	The delegation of one or more IT-intensive business functions/ processes to an in-house/ internal provider who in turn, owns, administers and manages the selected functions / processes, based upon defined and measurable performance metrics

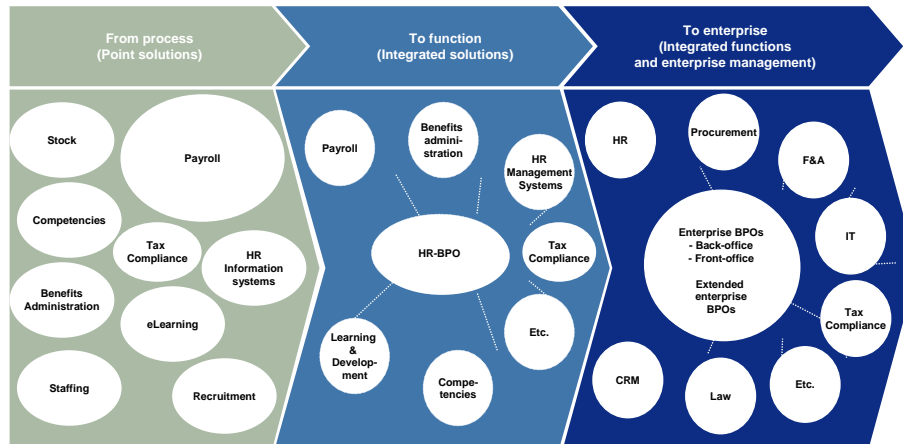


© 2007 KPMG LLP, a U.S. limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International, a Swiss cooperative. All rights reserved. Printed in the U.S.A.

3



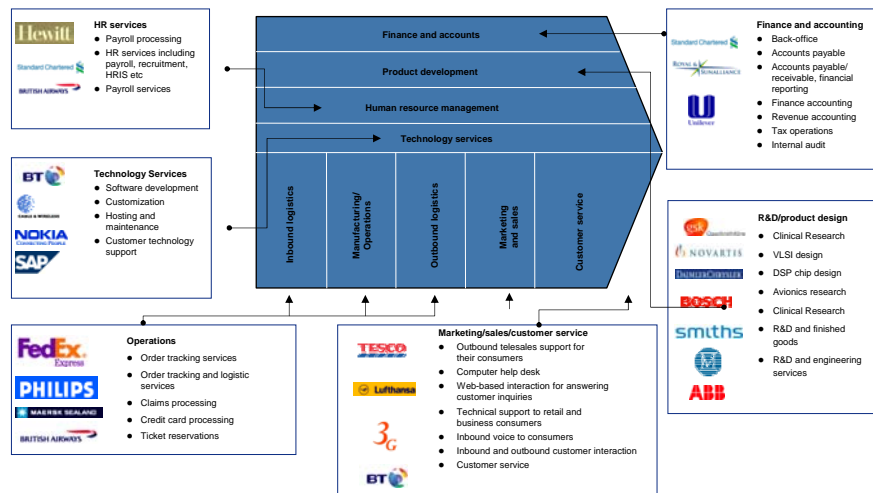
## Outsourcing market evolution – the future: from process to enterprise management



What is your situation?



## Some firms have taken the lead and already sourced successfully



Based on general public information





## Sourcing Trends

Sourcing is an integral part of modern corporate structure

- Efforts to reduce costs
- Access to new talent
- Enhance service level
- Gain operational efficiencies



## Personal Information and Outsourcing

- Personal information plays a key role in multiple business processes
- PII is stored in many corporate systems and Data repositories
- Every decision to outsource a process or activity may involve transfer of PII from the organization to third parties
- Ability to access information and/or view it (even if the information is still stored within the organization walls) may be considered a transfer to third party by some of the laws
- Organizations want the flexibility to optimize their structure and operations without being limited by current privacy legislation
- Data subjects expect organizations to provide the same level of protection to their information as committed when the data was collected and use the data only for the purpose stated in the notice.





## Risks

- Threats to brand and business that can be caused by privacy mismanagement are becoming a board and C level management issue. As a result, organizations are recognizing the need to ask tougher questions about the privacy and data handling practices of the business partners
- Privacy risks in outsourcing countries – many popular outsourcing countries do not have national privacy laws. Vendors there may not maintain privacy, security and data handling practices consistent with the banks that hire them
- Due diligence is essential to help ensure vendor's privacy practices are in synch with banks practices and expectations. Monitoring and auditing are critical.
- Regulators – Established formal guidelines on their expectations in the event of outsourcing
- Customers – See the entity that collected their data accountable for any future issue
- Media – Focus on the "big names"



## The Impact of Outsourcing





## The Current Environment

- Corporate governance structures are examined under a microscope.
- Management needs to minimize many types of risk, including privacy risk.
- Outsourcing business processes is commonplace, both domestically & off-shore.
- Attention increasingly focuses on the quality, or lack thereof, of third-party data processors.



## The Risk – Off-shore Outsourcing

Offshore outsourcing activities may occur without the organization for which the data is processed ever knowing it actually occurs

- UCSF medical transcript case
- Australian Outsourcing data breach





## Who controls the data?

- Service Providers – Data processed in hosted systems
- Business Process Outsourcing (BPO) – Data typically resides on the client's infrastructure – limited access is provided to vendor
- Application development – Data needed for testing by developers
- Data Center hosting, IT management outsourcing – vendor has more access & may have control over data
- Service Oriented Architecture – an evolving challenge



## Suggested Approach



## What do we see in the market

- More organizations are exercising the "Right to Audit"
- Vendors are audited multiple times
- Drive for independent third party audits
- Vendor assessment programs
  - Standard audit plans
  - Questionnaires
  - Risk based approach – rank vendors based on
    - Volume
    - Sensitivity
    - \$ involved
  - Roll out audit plan based on risk



## Vendor Governance and Oversight

- Understand your vendor:
  - What services do they provide you?
  - Where are they located?
- Look for the weakest control link – internal, vendor, subcontractors
- Pre- selection Considerations
  - Risk criteria – applied at contract level
  - Due diligence requirements
  - Controls Assessment
    - Security
      - Information
      - Personnel
      - Site
    - Business Continuity
      - Policy
      - Regulatory requirements







## Vendor Governance and Oversight, continued

- Perform risk assessment of vendors
- Contract Negotiation Considerations
  - Right to audit
  - Information protection
  - Background checks
  - Encryption
  - Decommission
- Post selection Considerations
  - Assessment responses
  - Re-assessment – frequency, type, scope
  - Onsite assessments? Who pays, who conducts?



## A Practical Approach

- Develop short form vendor assessment forms
- Develop/update standard template of contractual safeguards
- Develop guidelines for data transfer protocols
- Enhance regular auditing and monitoring
- Automating processes
- Vendor Privacy Practices and Safeguards to consider:
  - Privacy policy
  - Communication and training
  - Privacy management
  - Privacy compliance
  - Choice and consent
  - Global compliance
  - Consumer/data subject redress





## A Practical Approach, continued

Vendor information security practices and safeguards to consider:

- Technical controls
- Physical security

Vendors history of incidents

Vendors incident response policy and procedures

Vendors program for compliance monitoring and auditing



## Requirements from US Financial Institutes

- Regulators consider the financial institution responsible for the vendor's activity
- Vendors may be required to follow the FTC safeguards rule or banking regulations rule
- Both rules require a written information security program
- GLBA specifically covers vendor management.
- Boards should be aware of vendor contract and due diligence process
- At a minimum, vendor contracts are subject to the examination process. In some cases, the vendor operations can be subject to examination process.





What should you do tomorrow?



18275-F1BOS

## 10 Critical Questions \*

- Who are the outsourcing organizations we contract with and where are they located?
- Precisely what data are we sending to, and receiving from, outsourcing organizations?
- Is the data “personal information,” and have we given notice to our customers of this data transfer?
- What are our exposures if the data (both sent and received) is improperly accessed, used or maintained?
- What data protection clauses do we have in these contracts?
- What evidence do we have that these outsourcing organizations protect our data as outlined in these data protection clauses?
- What processes are in place to monitor the outsourcing organizations?
- Do these organizations outsource any of their processes in which our data may be further transferred to another organization?
- What processes do the outsourcing organizations we contract with use to verify the data protection practices followed by their outsourcing partners?
- What are the applicable privacy laws and regulations?

\* Developed by the AICPA/CICA Privacy task force



© 2007 KPMG LLP, a U.S. limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International, a Swiss cooperative. All rights reserved. Printed in the U.S.A.

21



## **Doron Rotman**

KPMG LLP  
National Privacy Service Leader  
Advisory

650-404-4176  
drotman@kpmg.com

