



## Pre – Reading

---

### *Outsourcing - Opportunities and Security Risks*



## SESSION 3

---

**Monday, November 7, 2005 – 12:30 - 17:30**

**Berne, Gurtenpark, Uptown**

---

An initiative to engage in strategic dialogue on IT security

**Microsoft®** **accenture**

---

With the support of





---

## MANAGEMENT SUMMARY

IT outsourcing is the delegation of IT services from a customer to an external service provider specializing in these services. Potential benefits of outsourcing are cost savings, improved quality of the outsourced services, and the opportunity of the customer to focus on its core competences.

The implementation of outsourcing often brings significant changes to the business processes and organization of the outsourcing company. To successfully plan and implement these changes is one of the main challenges in outsourcing. Other significant challenges have their origin in information security. A main source of challenges here is that the company that has outsourced IT services remains, often regulatorily, liable for information security, whereas some parts of its IT infrastructure are under the control of the service provider. A failure to meet any of the above challenges can have consequences that eliminate the anticipated benefits of outsourcing.

At the upcoming Swiss Security Exchange we will discuss the opportunities and risks of outsourcing, separately considering, from the business and the technical perspective, the risks for each of the phases (i.e., the preparation, the transition, and the operations phase) of the outsourcing process.

---

## OVERVIEW AND SOME FACTS

IT outsourcing is the delegation of IT services to an external service provider specializing in these services. Sometimes also a significant amount of management control is transferred to the service provider. Potential benefits of the outsourcing customer include:

- Cost savings
- Improved service quality of the outsourced operations
- Greater ability for the outsourcing client to focus on its core competencies

In general, the service provider's motivation is to make a profit. Yet, there are some providers whose motivation is to optimize the utilization of their IT infrastructure and thereby to reduce costs.

Important characteristics of an outsourcing deal are the scope of the services being outsourced and the country in which the service provider is located. The scope typically consists of a combination of the following services:

- Infrastructure management (e.g. management of servers, storage, and entire datacenters)
- Application management
- Desktop management
- Data management
- Support services (e.g. hardware maintenance)
- Network management
- Business processes (e.g. payroll, human resources, accounts receivable, shipping, insurance claims processing, etc.)
- Application development
- Systems integration



- Help desk
- Operational security (e.g. firewall monitoring, IDS monitoring, etc.)

A distinction in the geographical location of the service provider is often made between near-shore (for Switzerland, this typically means Eastern Europe) and off-shore (e.g., India) outsourcing. The latter is usually more cost effective, but also requires bridging a larger “cultural gap” (e.g., different legal systems, languages, social habits etc.).

The following findings from a recent survey by Forrester give a good picture of the status of the European outsourcing market:

- There is a significant diversity concerning the size and number of outsourcing deals across Europe. The UK and Germany are leading with respect to both number and value of deals. Switzerland figures towards the bottom of the table in number of deals, but ranks number four in size of the deals.
- Around 50% of the deals are in the financial services and government sectors.
- Deals initially typically last 5 years.
- Infrastructure outsourcing was ranked the number one service: more than two-thirds of the outsourcing deals contained infrastructure management. Application management came in second place. On the other hand, business process outsourcing and offshore outsourcing have not taken off yet.
- Swiss companies were found to be risk-averse, and observed to feel more comfortable closing deals with smaller service providers than with large ones.

---

## OUTSOURCING CHALLENGES

### ***General challenges and risks***

An inevitable consequence of outsourcing is that certain business and technology processes have to be implemented across the boundaries between the geographically separated customer and service provider. For processes to properly function in this setting, they have to be adequately designed and documented. Outsourcing clients will also need to design and document their processes in order to assert appropriate service levels associated with these processes.

Implementing these processes that span oceans, time zones, customers and service providers requires the creation of new job roles and supporting functions and changing existing job roles. At the same time, many jobs move from the customer to the service provider and some employees will lose their jobs. These significant process and organizational changes are among the most critical issues encountered in outsourcing.

The resulting changes are implemented in what we call the outsourcing process. A possible way to implement the outsourcing process is in the following phases:



1. *Scoping and planning before speaking to a service provider.* The potential customer engages in the following activities:
  - Determination of the outsourcing objectives, e.g., deciding whether the outsourcing objective is to reduce costs or to improve service quality.
  - Definition of the scope of the outsourced services.
  - Definition of measurement criteria that will assess whether the outsourcing project is meeting its objectives.
  - Self-assessment of outsourcing readiness, e.g., How mature are the customer's existing processes? Are there enough skills and manpower within the company to tackle the outsourcing process?
  - Make the business case and take the decision whether to outsource or not.
2. *Selecting a service provider*
  - Creating a short list of service providers.
  - Choosing the best provider.
3. *Working with your service provider to plan for rollout:*
  - Creating specific criteria for understanding whether specific services are meeting the customer's desired service levels.
  - Plan financial break-even point, possibly including opt-out points and strategies.
  - Planning of organizational and process changes.
  - Planning of IT infrastructure changes, e.g., data center move (i.e., transfer and integration of infrastructure, software, and data, from the customer's datacenter to the service provider's).
4. *Transition:* Implementation of process, organizational, and technology changes.
5. *Operation:* Outsourcing is established and the daily business is running. Modifications to the services are handled through change management processes.

Companies that are well-organized and well-operated before the outsourcing, usually face fewer challenges during the outsourcing process than less-organized ones. For the latter, it's important not to see outsourcing as an opportunity to get "your mess for less," but as an opportunity to improve their organization and processes.

Companies often focus on the evaluation of the service provider and the risks associated with the operation phase of outsourcing while neglecting risks that arise from an insufficient planning phase. Companies that do not understand this are rarely going to realize outsourcing benefits.

### ***Information security specific challenges and risk***

A study by Forrester has revealed that information security concerns are the main reason for the decision not to outsource. In the following, we shall see that there is in fact a series of security challenges related to outsourcing.

First we note that the observations and challenges that apply to outsourcing in general, as discussed in the previous section, also apply to information security



in outsourcing. In fact, a recent study by Forrester has found that security functions undergo a rather drastic organizational change in outsourcing. Thereby both, customers and service providers need to establish the new roles of “security managers for outsourcing” and supporting functions. Moreover, the implementation of security controls calls for a quite close collaboration across company boundaries between the customer and the service provider. The actual amount of collaboration necessary and the resulting challenges depend on the scope of the security controls being outsourced. As an example, virus scanning and vulnerability management are security controls that service providers can handle with little interaction with the customer. On the other hand, business continuity planning, incident management, and review / audit (of the service provider) are security controls that require considerable interaction between the outsourcing partners.

Additionally, there is a series of outsourcing-specific information security challenges. Most of them arise from a key principle concerning security in outsourcing; namely, the principle that *liability for information security cannot be outsourced*. This principle is part of many regulations, and in particular, part of the Swiss Federal Banking Commission’s circular concerning outsourcing. It also applies beyond regulatory requirements, e.g., when it comes to damages of a company’s reputation caused by security incidents. The principle imposes at least two fundamental requirements with regard to the implementation of information security in outsourcing:

- The customer must be able to determine the type and level of security controls that are operated by the service provider.
- The customer must be given the possibility to audit and review the implementation of security controls by the service provider. This requirement is, as an example, explicitly stated in the Swiss Federal Banking Commission’s circular.

It seems to be quite clear that a customer with poor information security know-how and processes will have difficulty meeting such requirements. There are also various challenges that arise when one tries to meet the above requirements:

- Reviews by outsourcing clients of their service providers must not breach the confidentiality of data and information on the infrastructure of that service provider’s other outsourcing clients. In addition, the service provider may be (rightfully) reluctant to reveal details about its own infrastructure and processes which it uses to manage its customers infrastructure. A possible way around this conflict is to engage a mutually trusted auditor to perform security reviews. Security certifications (e.g., BS 7799) of the service provider can serve as additional evidence for the quality of the security related services being provided. Yet, they cannot replace audits and reviews by the customer. In any case, it is important that review and audit rights are established in the outsourcing contract.
- It is not for all security controls an easy task to specify and monitor the appropriate service levels. For example, it is relatively easy to agree on service levels for the availability of systems, backup, and virus protection, but much more difficult for more demanding services, such as intrusion detection and prevention.

Additional complexity arises because the customer’s infrastructure is embedded in the service provider’s infrastructure. (For instance, an



outsourcing client's mail server is accessed and operated from the service provider's management consoles.) Thus, an outsourcing client has to make sure that the service provider's measures to secure its own infrastructure are adequate for providing the level and quality of security services the outsourcing client desires.

Last but not least, there are various outsourcing-specific sources of information security threats. Examples are:

- > Shared infrastructure for multiple clients.
- > Differences in the legal systems of the outsourcing client's and the service provider's countries.
- > Subcontracting to additional service providers with inadequate security controls by the service provider.
- > Contracting parts of the same business process to two different service providers can introduce additional risk.
- > Bankruptcy of the service provider.
- > Acquisition of the service provider by another company with different priorities.
- > Compromised employees at the service provider who reveal the customer's confidential information.

## **THE WORK SESSION AT THE UPCOMING SWISS SECURITY EXCHANGE**

---

The goal of the work session at the upcoming Swiss Security Exchange is to identify and understand the opportunities and risks of outsourcing. To this end we separately consider, from the business and the technical perspective, the risks encountered in each of the phases of the outsourcing process.



## **BUSINESS DECISION MAKERS CONFIRMED FOR November 7<sup>th</sup> (by October 27<sup>th</sup>)**

<b>Abdelhamid Usama</b>	Senior Architect IT Security, Ciba Specialty Chemicals
<b>Blackman Kevin</b>	Chief Technology Officer, Wisekey
<b>Braun Thomas</b>	IT Security Officer, World Trade Organization
<b>Eggel Damian</b>	Chief IT-Security Officer, Mobiliar
<b>Haering Kurt</b>	President, EFSI AG
<b>Halbheer Roger</b>	Chief Security and Privacy Advisor, Microsoft Schweiz
<b>Hämmerli Bernhard</b>	Vice President FG Sec School of Engineering and Architecture Lucerne (HTA)
<b>Hörler Andreas</b>	Head Information Security Management, Winterthur Insurance Group
<b>Koch Stéphane</b>	competitive intelligence & information security advisor, intelligenzia.net
<b>Lubich Hannes P.</b>	Principal Consultant Security, Computer Associates
<b>Kulhavy Vladimir</b>	Project Manager / Consultant / DS, Siemens Business Innovation Center
<b>Markwalder Peter</b>	Chief Security Officer and QM, Abraxas Informatik AG
<b>Messerli Daniel</b>	Chief Security Officer, Eidgenoessisches Justiz- und Polizeidepartement
<b>Nelißen Josef</b>	Chief Security Officer, ABB
<b>Olsen Rainer</b>	Head of IT Security, Credit Suisse Group
<b>Schenk Marc-André</b>	Group Information Security Manager, Nestlé
<b>Straub Wolfgang</b>	Dr. iur. Advocate, Deutsch Wyss & Partner
<b>Toggweiler Daniel</b>	Head of Telematic Services, The Swatch Group Ltd
<b>Trenta Giampaolo</b>	Group Chief Security Officer, Julius Baer & Co. Ltd
<b>Wuchner Andreas</b>	Head of Global IT-Security, Novartis Pharma AG
<b>Vogt Stefan K.</b>	Group IT Risk Management, Zurich Financial Services
<b>Zbinden Reto</b>	Director, Swiss Infosec
<b>Zuckschwerdt Markus</b>	Chief Security Officer, Galaxis AG

## **ORGANIZATION**

### **Executive Producers Swiss Security Exchange:**

<b>Christian Nagler</b>	Accenture
<b>Endre Bangerter</b>	Accenture
<b>Andrea Müller</b>	Microsoft GmbH
<b>Roger Halbheer</b>	Microsoft GmbH

### **Facilitator:**

**Laura Koetzle**, Vice President Research Forrester Research

Laura is vice president and research director of Forrester's Computing Infrastructures and Security group. Her primary areas of research include IT security and systems management. She also maintains research interests in enterprise application integration (EAI), Java 2 technologies, and software development methodologies.

She works with Forrester's clients to solve technical, strategic, and organizational IT security and systems management problems. She has redesigned network topologies, helped choose and implement systems management tools, created new IT security incident response procedures, and reorganized IT security and systems management groups.

Laura's work has enjoyed wide exposure in the media, including The New York Times, The Wall Street Journal, Business Week, and The Economist. Laura has also appeared on CNN, CNBC, CBC, and Reuters Television, and she is a frequent speaker at national and international executive conferences.

### **Previous Work Experience:**

Prior to joining Forrester, Laura was a senior technologist at Razorfish, a New York consultancy, where



she led teams of software developers responsible for eCommerce fulfillment systems, wireless content delivery applications, and real-time trading system interfaces for Fortune 500 clients. Before working at Razorfish, Laura built XML content management systems at PC World Communications in San Francisco. While living in Buenos Aires, Argentina, Laura worked as a translator.

**Education:**

Laura holds an A.B. in literature and a certificate in Latin American studies from Harvard University. She also attended the University of Buenos Aires.