Introduction
The decision to outsource is often made in the interest of lowering the Organizations cost, redirecting or conserving energy directed at the core competencies of a business, or to make more efficient use of worldwide labour, capital, technology and resources.

To keep control the security of the Organization's information and information processing facilities should not be reduced by the introduction of external IT Service Providers. This is needed to protect the accountability of the organization which can not be outsourced.

If an Organization does not understand the risk it faces (Due Diligence) and it does not implement the proper Information Security controls (Due Care) it can be legally charged with negligence and held accountable for any consequential loss of that negligence. This is formalised in an increa-

Highlights
- Preparation is the Key
- Accountability can not be outsourced
- There is a risk of a “gap” at the Tactical layer
- A Shared ISMS should prevent the occurrence of this “gap”
- IBM Security Consultants can help with implementing the Shared ISMS

To what extend Information Security can be outsourced?
To discuss to what extend Information Security can be Outsourced we look at the 3 Security Layers that can be thought of as a structure for Information Security, Strategic, Tactical and Operational information security.

The top layer outlines the management strategy called Information Security Governance. At this layer management should actively support security within the Organization through clear directions, demonstrate commitment, explicit assignment, and acknowledgement of Information Security responsibilities¹

At the Tactical layer Information Security Management is one of the IT Service Management processes. Every aspect of IT Service Management has Security Management considerations. There is a specific relation with Availability Management and through this Business Continuity²

Managed Security Services can be delivered by the IT operations departments of the Organization or by external third parties. An independent decision can be made for each service to in- or outsource. Multiple providers can be selected to deliver Managed Security Service.

1 ISO 27002 6.1.1 Management commitment to information security
2 ITIL Security Management
Selecting a Service Provider

When selecting a Service Provider for IT Security Outsourcing services there are two different views to consider based on the two-fold goal of the Information Security Management process as defined by ITIL.

From the point of view of the Service Provider as defined by ITIL the goal of the Information Security Management process is two-fold:

- First to meet the *internal* Information Security requirements. (To assure the IT Service Provider’s own continuity). These are the Service Providers own internal requirements. This view is looking at the quality of the providers Information Security Management System to assure the IT service provider’s own continuity.

- Second to meet the *external* Information Security requirements. (SLA’s, contracts, legislation, policies). These are the requirements from the Organization to the Service Provider. This view is to consider how the provider will guarantee that adequate Information Security, as defined by the Organizations Risk Assessment, will be maintained, and how security will be adapted to identify and deal which changes to risks.

**Shared ISMS**

A Shared ISMS should prevent the occurrence of a "gap" between the Operational baseline Information Security of the providers Service Catalogue and the control objectives defined during the Organizations Risk Assessment taking into account its business risk appetite.

To implement a Shared ISMS, an Information Security Tactical management board as part of the ISMS is recommended to facilitate the implementation and operation of the Shared ISMS.

**Shared Information Security Plan**

Because of the shared nature of the implementation and operation of the ISMS as explained it is recommended to have a Shared Information Security Plan (risk treatment plan) in addition to the contract which is maintained between both parties.

**Steps to take in an outsourcing engagement**

For the steps to take in an outsourcing engagement, specific one time security in outsourcing knowledge is needed to prevent some of the common pitfalls discussed. External consultancy can help to provide this knowledge.

**Step1:** Preparation is the Key: Pre Outsourcing Security Assessment => RFP

**Step2:** Evaluate and Select a Service Provider: Provider assessment

**Step3:** Setup the contract: legal advice

**Step4:** Transition and Transformation: Peak load because of BAU and TRN/XFM effort, can be handled by external program management.

**Step5:** Business as usual: Assessing the governance organization and/or the Service provider.