IBM Global Technology Services

Outsourcing and Information Security

Preparation is the Key
However ultimately accountability cannot be outsourced

February 2009

1. Introduction 3
- 1.1 Reason for outsourcing 4
- 1.2 Main Outsourcing issue 4

2. To what extent can Information Security be Outsourced? 5
- 2.1 Information Security Governance 6
- 2.2 Outsourcing Information Security Management 7
- 2.3 Managed Security Services 7

3. How to select a Service Provider? 9
- 3.1 Internal Information Security requirements 9
- 3.2 External Information Security requirements 10
- 3.3 Include Information Security Projects 11

4. Shared Information Security Management System 12
- 4.1 Plan: Establish the ISMS 13
- 4.2 Do: Implement and operate the ISMS 13
- 4.3 Check: Monitor and review the ISMS 15
- 4.4 Adjust: Maintain and Improve the ISMS 15

5. Shared Information Security Plan 16

6. Transition / Transformation 18
- 6.1 Information Security Transition 18
- 6.2 Transformation 19

7. Steps to consider in a Outsourcing engagement 20

8. Conclusion and Useful Information 21

9. Glossary 22

1. Introduction

The objective of this whitepaper is to discuss some important Information Security management issues Organizations face when they are considering, or are in the middle of, Outsourcing their ICT environment to an external Service Provider. The issues discussed here are mostly related to closing or preventing the "gap" between Information Security Operations and business strategy and how to ensure that the proper identification of, assessment of and action on risk events takes place within the Outsourced environment.

The target audience of this whitepaper are professionals with Information Security responsibilities within an Organization, such as Security Officers and Security Managers. Security consultants or specialists from Service Providers may be interested in this whitepaper from a service delivery point of view. Finally, the Risk and Compliances professionals from the Outsourcing Organization, the Service Provider or independent auditing/assessment firms can read the whitepaper from a Risk and Compliances point of view.

This whitepaper uses the ISO/IEC 27001 (and ISO/IEC 27002) international standard for an Information Security Management System as reference. Some basic knowledge of the ISO/IEC 27001 information security terminologies is assumed.

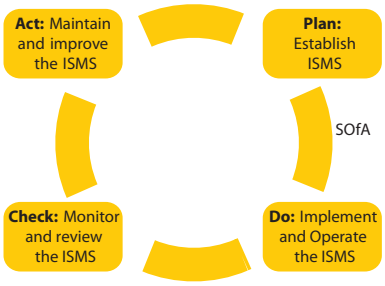

Figure 1 Plan-Do-Check-Act

ISO/IEC 27001 is an Information Security Management System (ISMS) standard published in October 2005 by the International Organization for Standardization and the International Electrotechnical Commission. Its full name is *ISO/IEC 27001:2005 – Information technology – Security techniques – Information Security management systems – Requirements*, but it is commonly known as "ISO 27001". This International Standard adopts the "Plan-Do-Check-Act" model, also called the Deming Cycle. This model is also used in this whitepaper. See Figure 1 **Plan-Do-Check-Act**.

In this document the term **Organization** is used for the legal entity that is contracting a Service Provider to deliver IT services. The **Service Provider** is the vendor delivering Managed Security Services or Outsourced Services to that Organization.

The issues discussed in this paper are:

- To what extent can Information Security be outsourced? (Chapter 2)
- How to select a Service Provider? (Chapter 3)
- Shared Information Security Management System (Chapter 4)
- Shared Information Security Plan (Chapter 5)
- Transition / Transformation (Chapter 6)
- Steps to take in an Outsourcing engagement (Chapter 7)

1.1 Reason for outsourcing

Outsourcing entered the business world in the 1980s and often refers to the delegation of non-core operations, from internal production to an external entity specializing in the management of that operation. The decision to outsource is often made in the interest of lowering company costs, redirecting to or conserving energy for the core competencies of a business, or making more efficient use of worldwide labour, capital, technology and resources.

Outsourcing IT to an external IT Service Provider can introduce additional threats to the Information Security of an Organization.

Example: *In April of 2005, a high-profile case involving the theft of $350,000 from four Citibank customers occurred when Indian call-centre workers in Pune, India, acquired the passwords to customer accounts and transferred the money to their own accounts opened under fictitious names. Citibank did not find out about the problem until the American customers noticed discrepancies with their accounts and notified the bank.*[1]

1.2 Main Outsourcing issue

Organizations who are (considering) Outsourcing their IT should maintain the Information Security of the Organization's information processing facilities that are accessed, processed, communicated with, or managed by external IT Service Providers. To maintain control, the security of the Organization's information and information-processing facilities should not be compromised by the introduction of external IT Service Providers. **This is needed to protect the accountability of the organization, which cannot be outsourced**.

If an Organization fails to 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 resulting from that negligence. This is formalized in an increasing number of laws and regulations that Organizations have to comply with.

Where there is a business need for Outsourcing IT to an external IT Service Provider, a Risk Assessment should be carried out to determine Information Security implications and control requirements. Controls should be agreed and defined in an agreement with the Service Provider. The provider should guarantee that adequate Information Security, as defined by the Risk Assessment, will be maintained, and the Provider should also indicate how Information Security will be adapted to identify and deal with changes to risk.

1 http://www.infoworld.com/article/05/04/07/HNcitibankfraud_1.html

Many Organizations find it difficult to extend their established Information Security Management System to their Service Provider, resulting in a "gap" between Information Security Operations and business strategy, between policy and practice, and between the Organization and its Service Provider. This will negatively influence the Organization's ability to effectively handle risk events (e.g. emergencies, incidents, fraud, etc.) and the Organization's compliance.

2. To what extent can Information Security be Outsourced?

The triangle in Figure 2 **Information Security Layers** shows the three layers that can be thought of as a structure for Information Security: Strategic, Tactical and Operational Information Security.

The Information Security Governance at the Strategy Layer cannot be outsourced because ultimate accountability always rests within the Organization itself. This is discussed in more detail in the section 2.1 Information Security Governance.

The Outsourcing of Information Security Management in the Tactical Layer is the area where often the "gap" between Strategy and Operations (i.e. between the Organization and the provider) can be found. Section 2.2 Outsourcing Information Security Management and the rest of the document will focus mostly on this layer.

The Outsourcing of operational Information Security activities to a Managed Information Security Services Provider is discussed in section 2.3 Managed Security Services.

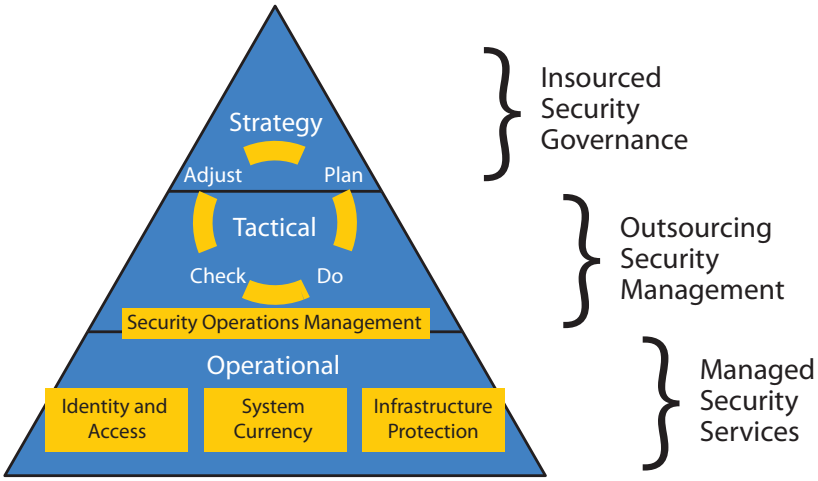

Figure 2 Information Security Layers

2.1 Information Security Governance

The top layer outlines the management strategy called Information Security Governance in this paper. In this layer *management should actively support security within the Organization through clear directions, demonstrated commitment, explicit assignment, and acknowledgement of Information Security responsibilities*.[2]

In this layer, the Risk Management process is executed as part of the established Information Security Management System (ISMS) see Figure 1 Plan-Do-Check-Act.

- **Risk Management:**
  - **Risk Assessment:** Overall process of analysis and risk evaluation.
    - Risk Analysis: Systematic use of information to identify assets and to estimate the risk.
    - Risk Evaluation: Process of comparing the estimated risk against given risk criteria to determine the significance of the risk.
  - **Risk Treatment:** Process of selection and implementation of measures (Controls) to modify risk.
  - **Risk Acceptance:** Decision to accept a risk

Based on the results and conclusions of the Risk Assessment and Risk Treatment process, legal or regulatory requirements, contractual obligations and the Organization's business requirements for Information Security, a Statement of Applicability (SOA) should be documented that describes the control objectives and the controls that are relevant and applicable to the Organization's ISMS.

Senior management of the Organization is ultimately responsible for Information Security of the Organization and the protection of its assets as they understand the vision of the company and the business goals. Therefore they cannot outsource the Information Security Governance Layer. When an Organization needs help with the Information Security Governance, help is available using Consultancy. An Organization should not make the mistake of thinking that an Outsourcing provider will solve this non-IT problem. Ultimately all consequences of not properly implementing Information Security are borne by the Organization and not the provider.

2 ISO 27002 6.1.1 Management commitment to information security

2.2 Outsourcing Information Security Management

In the Tactical layer, Information Security Management is one of the processes that is executed by an Organization as part of IT management. In an IT Outsourcing situation, the execution of those processes is done by an external IT Service Provider. This is the case for the Service Support processes at the Operational level (Incident Control, Change Management, etc.) and for the Service Delivery Processes (Service Level Management, Availability Management, etc.) at the tactical level. *Every aspect of IT Service Management has Security Management considerations. There is a specific relation with Availability Management and through this Business Continuity*[3].

It is at this level that the "gap" between the Service Provider and the Organization itself often occurs at the interface between the two. To prevent this "gap":

- Operational processes deployed by the Service Provider should be in line with the appropriate laws, regulations, best-practices and risk-appetite policy determined in the strategy layer;
- Risk (and non-compliance) events should be properly identified and assessed;
- Action and reporting should take place in a structured manner.

It is therefore necessary to carefully select a Service Provider and implement a shared Information Security Management System with this Service Provider. The next chapters will cover these topics.

2.3 Managed Security Services

Managed Security Service can be split into three main Service lines:

1. Identity and Access: This service line encompasses Information Security controls that provide access to a system or infrastructure. These controls provide identification, authorization and access to information resources. Although Identity and Access can be seen as part of the business processes, many of the activities that are part of this Service Line are very operational and can be outsourced to Service Providers. Therefore this Service Line is part of the Operational layer.

2. System Currency: System Currency Services represent Information Security controls that are targeted at a specific system or application. For example, a control that hardens a specific server would be considered to be within this service. These controls have a direct and indirect impact on the data and resources specific to that system or application.

3 See ITIL Security Management

3. Infrastructure Protection: This service line encompasses Information Security controls that are not specific to a given system or application, but rather are targeted at the facilities or network level. These controls provide issue detection, reporting and remediation for the given facility or network.

Managed Security Services can be delivered by the IT operations departments of the organization or by an external third party. There are a lot of Managed Security Services available in the market. Often those services are based on a specific technical solution. As a result, the services can be provided independently from each other. This makes it possible to:

1. Make an independent decision for each service to insource or outsource it;
2. Use multiple providers to deliver Managed Security Service.

Information Security Management at the Tactical level still has to coordinate and integrate all Information Security services provided to the Organization.

A typical situation for considering the Outsourcing of a Managed Security Service is when an organization wants to introduce a new technical Information Security control, but does not have the skills to implement this in an efficient way. This would be the moment to look for external third parties who can deliver the required technical Information Security control in a more efficient way than the organization itself can.

An example of this would be the decision to implement an abnormally based Intrusion Prevention System because of recent Zero Day exploits. In these cases, the speed of implementation and required adjustments in connection with new vulnerabilities may also be a consideration in a decision to outsource these services to external service providers.

3. How to select a Service Provider?

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 **external** Information Security requirements. (SLAs, contracts, legislation, policies). These are the requirements from the Organization to the Service Provider.
- Second to meet the **internal** Information Security requirements. (To assure the IT Service Provider's own continuity). These are the Service Provider's own internal requirements.

The IT Service Provider selected should provide good quality in meeting its *internal Information Security* requirements. This can be achieved by selecting a provider that can show results of an independent review of their Information Security Management System. An ISO 27001 certificate or a SAS70[4] type II report are examples of this. One should be aware that these certificates are issued for generic services and not for customer-specific requested services.

Furthermore, this will not say anything about the quality of how the *external Information Security* requirements are met (read the organizations requirements). For the *external Information Security* requirements, a provider should be selected that has an efficient and flexible approach in providing Information Security based on the external Information Security requirements and that offers a shared Information Security Management System to meet both set of requirements. The concept of shared Information Security Management System is explained in Chapter 4.

3.1 Internal Information Security requirements

A contract with an IT Outsourcing provider often encompasses a period of 5 to 7 years, and the Organization's business depends strongly on the continuity of the service provision. It is therefore key to select a provider with a high-quality approach to managing Information Security. It is also advisable to select a provider that has a proven and stable track record of providing these services over a number of years.

The Provider's approach to managing Information Security and its implementation should be reviewed independently at planned intervals, or when significant changes to the Information Security implementation occur.

An ISO 27001 certificate or a SAS70 type II report are examples of independent reviews of the quality of the provider's Information Security Management Systems.

4 http://www.sas70.com/

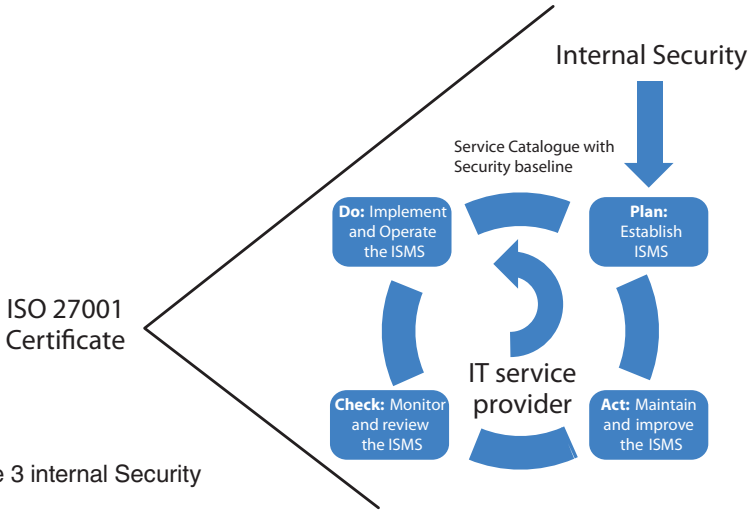

Figure 3 internal Security

Note that the result of such an independent review does not say anything about the external Information Security requirements. The provider was not aware of specific control objectives applicable to its clients when it selected the controls to be implemented and reviewed. In the best case, the set of controls selected by the provider will be targeted to a specific industry or to specific regulations. This will result in an Information Security baseline, establishing a basic level of Information Security for the Service Catalogue the provider is offering.

3.2 External Information Security requirements

When selecting a provider for Outsourcing, it should be considered how the provider will guarantee that adequate Information Security, as defined by the Organization's Risk Assessment, will be maintained, and how security will be adapted to identify and deal which changes to risks.

The Service Provider should be asked what their Risk Treatment plan is in order to achieve the control objectives the organization has defined during its Risk Assessment (SOA). It should also be considered how the effectiveness of the controls is measured in order to determine how the controls achieve the planned control objectives.

Figure 4 External Security

A common pitfall in the Service Provider selection process is that an Organization only compares the Information Security baselines of the different Service Providers. By doing so, you will not know how the provider will implement and operate the ISMS derived from the Organization's specific Risk Assessment.

Preparation before outsourcing is key.

The best way to select a provider for Outsourcing is to use the Organization's existing Information Security governance framework to do a Risk Assessment on the upcoming Outsourcing situation in order to determine the controls that are required on the part of the provider. The Service Providers can then be compared based on the set of required information Security Controls. Be aware that Outsourcing a set of controls will differ from the situation before the outsourcing, because outsourcing itself may introduce new threats and vulnerabilities. An example of such a new threat can be personnel that are dissatisfied about their transfer from the Organization to the Service Provider. Vulnerabilities can, for example, be introduced by the additional network connections to the Service Provider needed to enable remote management of the systems.

When an Organization is not confident about their current Information Security governance framework or about determining the specific risks introduced by Outsourcing, a pre-Outsourcing Security assessment can be conducted by an external consultancy company to help identify weaknesses and to provide guidance in defining and implementing the Information Security Governance. Do not rely on the Outsourcing provider to solve any of the problems an Organization might have with Information Security Governance after signing the Outsourcing deal.

3.3 Include Information Security Projects

The selection process from the moment the decision to outsource is made to the actual start of the Transition will often take a lot of time, sometimes up to two years. For the Organization it is very tempting to postpone investments in Information Security projects for that period. From a financial point of view this can be a good decision. However, after the Transition of responsibilities to the Service Provider, these projects still have to be executed. The best approach is to identify those projects and to include them in the RFP. This way it will be clear to the Service Provider which projects they have to deliver during Transformation and the Organization can compare the proposals of the Service Providers in the selection process.

Not including these projects in the contract will lead to discussions about the financing of such projects later on. By that time Organization and Service Provider will already be committed to each other. The cost calculated by the Service Provider at that time will probably be less competitive than in the negotiation phase of the contract.

Also, postponing the investments and not addressing them adequately will significantly increase the risk the Organization is exposed to by not being prepared for (new) vulnerabilities.

4. Shared Information Security Management System

" The risks to the Organization's information and information processing facilities from business processes involving external parties should be identified and appropriate controls implemented before granting access."[5]

When an Outsourcing provider is selected, the Organization and the provider need to work on establishing a Shared Information Security Management System (ISMS). This Shared ISMS should prevent the occurrence of a "gap" between the Operational baseline Information Security of the provider's Service Catalogue and the control objectives defined during the Organization's Risk Assessment, taking into account its business risk appetite (the amount of business risk the Organization is willing to accept according to its business model).

As you can see in Figure 5 **Shared ISMS** this will lead to a shared implementation and operation of the ISMS. The Plan-Do-Check-Act cycle will remain separate and distinct responsibilities for the Organization and the IT Service Provider. In the next sections, the Plan-Do-Check-Act cycle is discussed in more detail.

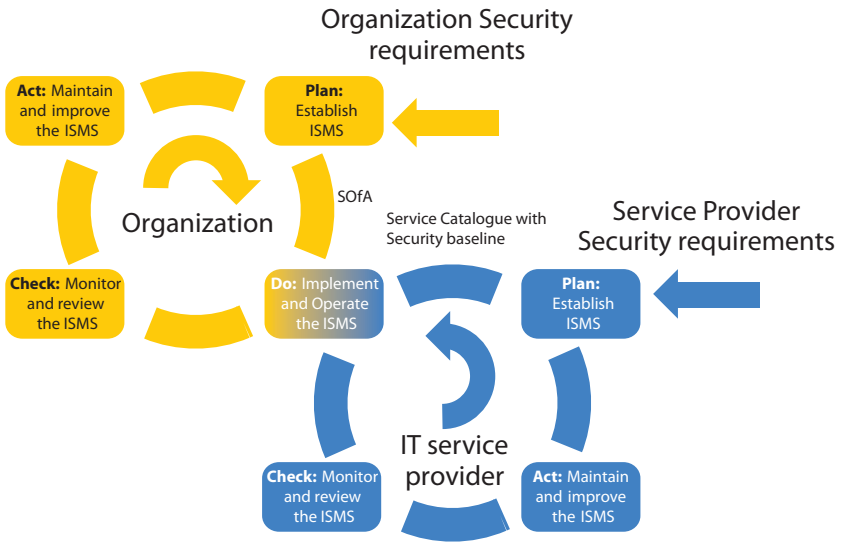

Figure 5 Shared ISMS

4.1 Plan: Establish the ISMS

Establish ISMS policy, objectives, processes and procedures relevant to managing risk and improving Information Security to deliver results in accordance with an Organization's overall policies and objectives. A Risk Assessment should identify, quantify and prioritize risk against criteria for Risk Acceptance and objectives relevant to the Organization. Business, legal and regulatory requirements should be taken into account.

If an Organization fails to 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 resulting from that negligence. This **accountability** cannot be transferred to the Service Provider and therefore the establishment of the ISMS should be retained within the organization as part of the Information Security Governance in the Strategic layer.

The Organization and its IT Service Provider may have totally different starting points from a business point of view when establishing their ISMS, both from their risk-appetite and regulatory perspectives. Think of an IT provider with an entry to the New York stock exchange (SOX compliant) providing service to a Dutch governmental Organization (this Organization needs to be compliant with the regulations on government information security (*Voorschrift Informatiebeveiliging Rijksoverheid*; VIR). Both should establish their own ISMS to fulfil the specific requirements based on totally different business models.

4.2 Do: Implement and operate the ISMS

Implement and operate the ISMS policy, controls, processes and procedures. This activity can largely be transferred to the Outsourcing provider for the scope of the agreement. In almost all cases some controls will remain outside the scope of the Outsourcing agreement. Information Security end-user training and knowledge is a common example of such retained control.

A clear allocation of Information Security responsibilities to the parties involved is needed to ensure coordination of Information Security activities between the Organization and the Service Provider. It is considered a management responsibility of the Organization to assign and coordinate the Information Security across the Organization. Therefore, Information Security Governance in the Strategic layer should be involved in this allocation of responsibilities.

Based on the SOA, Information Security baseline and the allocation of responsibilities, the Outsourcing provider should maintain an Information Security plan (this is called the Risk Treatment Plan in ISO/IEC 27001). This Information Security plan should be periodically validated by management of the Organization as part of its commitment to Information Security in the Information Security Governance layer.

To implement a Shared ISMS, an Information Security Operation management board as part of the operation of the ISMS is recommended. On this board, communication on Operational Information Security follows a pre-defined meeting structure and schedule to facilitate a clear understanding of the dependencies in a Shared ISMS. Figure 6 shows an example of such a shared board meeting structure.

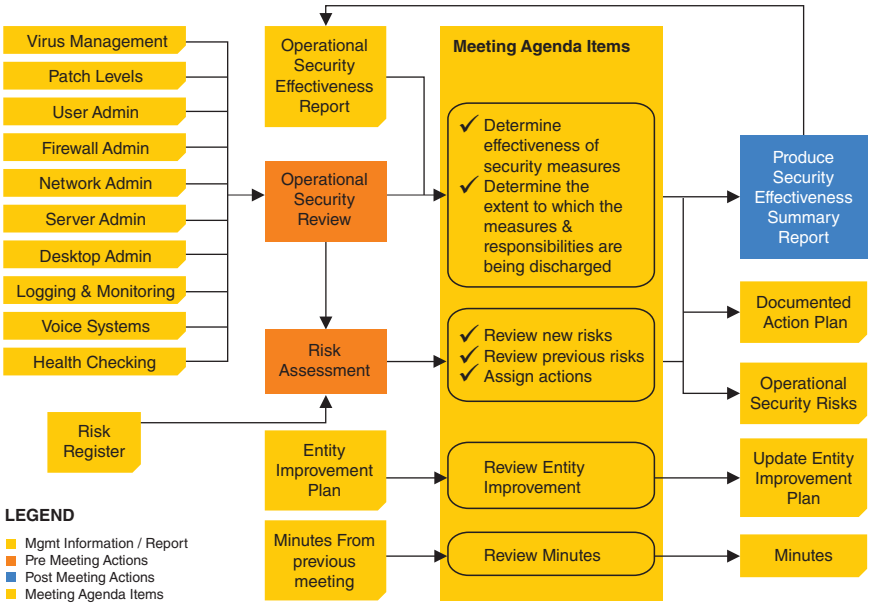

Figure 6 Example of an Operational Information Security Board meeting structure

For such a meeting structure it is important to get participants with an equal mandate in their own environments. This is to make sure that decisions made by this board have the support of both the Organization and the Service Provider. It will not work when an IT Security Specialist of the Service Provider is meeting with the CISO of the Organization. When more than one Service Provider are involved, they all should be on the board to make sure that all operational Security issues are properly addressed by the right party.

When the Organization's Operation is split up into multiple regions or business units, consider having multiple local boards reporting to one global board. This will enable local flexibility within a global framework.

4.3 Check: Monitor and review the ISMS

Assess and, where applicable, measure process performance against ISMS policy, objectives and practical experience and report the result to management for review.

As you can see in Figure 5 **Shared ISMS** there are two checks taking place. On the one hand, the IT Service Provider is reviewing against their Information Security baselines and internal Information Security objectives, and on the other, the Organization is reviewing against the SOA and the *external* objectives. Both actions are depicted as separate responsibilities for the same reasons as described in section 4.1 Plan: Establish the ISMS: The IT Service Provider might have different compliancy objectives than the Organization.

Note: this is about monitoring and reviewing (auditing) the ISMS and not operational Information Security monitoring as, for example, the monitoring of access logs. This is considered part of the operation of the ISMS as discussed in the previous section.

4.4 Adjust: Maintain and Improve the ISMS

Take corrective and preventive actions, based on the results of the internal ISMS audit and management review or other relevant information, to achieve continual improvement of the ISMS.

These adjustment activities are part of the Information Security Governance in the Strategic layer and therefore should not be outsourced. This activity will receive input from the independent reviews in the Check phase and SLA reports from the Do phase. Based on this information, together with changes in the business environment, the Risk Assessment should be updated to identify needed changes in the Information controls that should be implemented.

The Outsourcing provider should participate in this activity. They can provide information on the cost and feasibility of changing or implementing new controls. They can also provide expertise on estimating the likelihood of an Information Security threat exploiting vulnerabilities in the Organization's IT. This information is needed to update the Risk Assessment. For this purpose a policy review board can be established.

5. Shared Information Security Plan

When a Service Provider is selected, take into account the considerations in Chapter 2: Information Security should be addressed in the contractual agreement with the Service Provider. ISO 27002 section 6.2.3. provides an extensive list of terms to be considered for inclusion in such a contractual agreement. Two additional contractual terms to consider are:

- Transformation projects to implement additional Information Security Controls to mitigate the additional Risk introduced by outsourcing or to improve the effectiveness of the current controls. Also include postponed investments in Information Security projects.

- Responsibility and cost consequences for both known and unknown non-compliance issues handed over from the Organization to the Service Provider. (see Chapter 6.1)

Because of the shared nature of the implementation and operation of the ISMS as explained in Chapter 4, it is recommended you have a Shared Information Security Plan (risk treatment plan), in addition to the contract, and which is maintained between both parties. The Information Security Plan is an operational document containing information on the ISMS policy, controls, processes and procedures required to be implemented and operated to protect both the Organization and the Service Provider's data and assets.

The Information Security Plan can be seen as a more flexible and detailed specification of the contract. Other input for this document is the Service catalogue with the Information Security baseline of the Service Provider and the SOA of the Organization. The Service Provider can maintain the document but the Organization's management should approve it. This is to enable the management to provide evidence of its commitment to the implementation and operation of the ISMS as required by ISO 27001 5.1.

It is suggested that the following items are specified in more detail in the Information Security Plan.

1. Allocation of Information Security responsibilities: All Information Security responsibilities should be clearly defined between Organization and Service Provider. Items to cover are:

    a. Security Policy
    b. Organization of Information Security
    c. Asset Management
    d. Human Resources Security
    e. Physical and Environmental Security
    f. Communications and Operations Management
    g. Access Control
    h. Information System Acquisition, Development and Maintenance
    i. Information Security Incident Management
    j. Business Continuity Management
    k. Compliance

2. Technical Controls to be implemented: Technical Specifications that describe configuration settings to enable or enforce the required controls.

3. Managed Security Service in scope: Some Operational Information Security activities might be retained or provided by some other third party.

4. Process interfaces: Information Security processes overlapping both the IT Service Provider and the Organizations should have clearly defined interfaces.

5. Approved exceptions: In some situations the IT Service Provider deviates from the Organizations Information Security policy. In such cases, a Risk Assessment should be conducted before allowing the Service Provider to deviate. The resulting approved exception should be documented.

6. Pre-defined meeting structure and schedule for the Operational Information Security management Board.

6. Transition / Transformation

After the contract has been signed between the Organization and the Service Provider, a Transition period is needed in which responsibilities for delivering services are transferred from the Organization to the Service Provider. This period will take typically about 3 to 6 months. At the end of this period, the service will be delivered in the same way as before the contract was signed, only now under the responsibility of the Service Provider.

After Transition, a 6-to-12-month period is typically defined in which improvement or Transformation projects are executed to increase the efficiency or quality of the services provided. During this period the delivery of the outsourced services will be transformed from the as-is situation, as handed over during Transition, to the new to-be situation, as agreed in the contract.

6.1 Information Security Transition

In the Transition phase security responsibilities are transitioned to the Service Provider. It is important that the Organization plans and manages the Transition to a Service Provider carefully to prevent the increase of the Risk to the business without identifying and evaluating options for the treatment of the risk.

Special attention should be given to non-compliance issues. There are always non-compliance issues at a given point in time in a complex IT environment. There will very likely be non-compliance issues within the scope of the outsourcing deal, both known and unknown. Known issues should be handed over to the Service Provider during Transition. In the contract, guidance should be given on how the costs of solving those issues will be handled.

There will also be unknown non-compliance issues handed over. To prevent discussions on the responsibility for and the cost of solving these issues when discovered later on in the life cycle of the contract, an Information Security Base or starting point should be established during the Transition. This Base can be considered a picture of the situation on the day that the Service Provider takes over the responsibilities. To create this Information Security Base, the Organization and the Service Provider work together to perform a technical (platform) review and to assess the Organization's security processes, roles and responsibilities. The Information Security Base will be used to identify gaps between the current Organization Information Security environment and the contracted future Security state. This gap will serve as the starting point for the Information Security Transformation program.

Some of the Information Security processes will be “broken” because actions will be transferred to the Service Provider and other actions will stay with the Organization. For those processes that overlap both the Organization and the Service Provide, clear interfaces should be defined to ensure continuation of the overall process. An example of this is the reporting of Information Security Incidents.

6.2 Transformation

During the Transformation Program, several types of Information Security-related projects are executed.

- During the creation of the Information Security Base in Transition, gaps or unknown non-compliance issues will be discovered. For each of these issues a Risk mitigation or Risk acceptance should be agreed based on a Risk Assessment. This project should be done in cooperation between the Service Provider and the Organization: the Service Provider identifying the issue and proposing mitigations and the Organization providing a Risk Assessment and making a decision on the mitigation.

- The Risk profile of the Organization will change because of the Vulnerabilities and Threats introduced by the outsourcing. Additional controls should be selected to bring the risk down to an acceptable level. During Transformation, projects to implement those additional controls will be executed. These projects should already have been identified in the contract.

- There will be other non-Information Security projects that will impact Information Security. Examples of this are the development of a new build or a server consolidation project. For these kinds of projects it is very important that the to-be Information Security requirements are known prior to the start of the project. This is to prevent the creation of new legacy.

- The Service Provider will often have some internal Information Security projects to transform the environment in scope, to the Internal Information Security requirements of the Service Provider. The Organization should be aware of those projects and should ensure that they will not increase the level of risk to their business.

- In the contract, agreements may be made to change and/or enhance existing Security solutions to better fit the Organization’s Security requirements. These are typically best executed as part of “the bigger” transformation scope instead of a separate project because the transformation governance structure can be used.

7. Steps to consider in a Outsourcing engagement

- **Step1: Preparation is the Key.**
    - The Organization should have an Information Security Management System (ISMS) in place to connect to the ISMS of the IT Service Provider to enable the implementation of a Shared ISMS.
    - A Risk Assessment should be done to determine the Security controls applicable for the new outsourcing situation.
    - An Information Security Base should be available to describe in detail the Security situation that is handed over to the IT Service Provider.
    - A RACI table should be created to define the division of the responsibilities between the Organization and the Service Provider.
    - Current and future Information Security Projects should be identified.

  One way to validate if an Organization is well prepared for an Outsourcing engagement is to conduct a **pre-Outsourcing Security Assessment** on the items above.

- **Step2: Evaluate and Select a Service Provider.**
  Based on the preparation in step 1, an RFP can be written that clearly expresses the Security requirements the Organization has of its Service Provider. This will enable the Organization to compare the proposals of the Service Providers based on the specific Security solutions the Providers are offering, and not only based on the Security of their standard Service Catalogue.

- **Step3: Set up the contract.**
  Creating a contract is often very much a lawyer's party. The clearer the RFP and the provider's response, the easier it will be for the lawyers to create a workable contract. Do not put specific Security Controls into the contract. This will make the Shared ISMS very inflexible when new threats or vulnerabilities occur. The details of the agreed Shared ISMS should be documented in a Shared Information Security Plan. This is a living document which should be reviewed at least yearly or when major changes occur.

- **Step4: Transition and Transformation**
  This phase can take more than a year. During this period, normal day-to-day Security management activities by the Organization are continued (the part that is not handed over to the Service Provider). In addition to this extra temporary effort is needed of the Organization:
    - The Organization's part of the Shared ISMS should be implemented during Transition

- During the Transformation program, Security-related projects that are executed by the Service Provider also require effort on the part of the Organization.

This effort should not be underestimated. Often there will be a peak in the additional workload required in de first period of the Outsourcing engagement. Therefore additional resources are needed.

A way to handle this peak load in the Organization's effort is to ask an external party to help with the Security Program management on behalf of the Organization.

- **Step5: Business as usual.**
  To improve the quality and effectiveness of the Shared ISMS, an independent assessment can be conducted to determine possible improvements in the cooperation between the Organization and the Service Provider(s).

8. Conclusion and Useful Information

" Preparation is the Key. However, Utimately accountability cannot be outsourced".

To discuss the issues raised in this paper, please contact:

Rob Meijer
Managing Security Consultant
E-mail: rob_meijer@nl.ibm.com
Telephone: + 31 20 513 95 39

For more information

Please visit: ibm.com/services/nl/bcrs

9. Glossary

Due Care:	Do all you reasonably can to prevent Information Security breaches.
Due Diligence:	Properly investigate all of the possible weaknesses and vulnerabilities of an Organization.
Information Security:	Preservation of confidentiality, integrity and availability of information.
Information Security Base:	Starting point of the Security State as handed over from Organization to Service Provider at the start of an Outsourcing contract.
Information Security Operations:	Activities involved in the running of an Information Security solution or service.
ISMS, Information Security Management System:	That part of the overall management system, based on a business-risk approach, to establish, implement, operate, monitor, review, maintain and improve Information Security. ITIL, IT Infrastructure Library.
Organization:	In this whitepaper the legal entity that is contracting a Service Provider to deliver ICT services.
Outsourcing:	Delegation of non-core operations from internal production to an external entity specializing in the management of that operation.
RACI:	Responsible, Accountable, Consult, Informed
RFP:	Request for proposal.
Risk Assessment:	Overall process of analysis and risk evaluation.
Risk Treatment:	Process of selection and implementation of measures to modify risk.
Service Provider:	Vendor of Managed Security Service or Outsourcing Service to the Organization.
SOA:	Statement Of Applicability.
Threats:	A potential cause of an unwanted incident, which may result in harm to a system or organization.
Vulnerabilities:	A weakness of an asset or group assets that can be exploited by one or more threats.

IBM Nederland BV
Johan Huizingalaan, 765
1066 VH Amsterdam
Nederland

BUW0309-NLEN-00