Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

A Security Guide For Acquiring Outsourced Service

Outsourcing is not an abdication of the organisation's security responsibilities to an external contracting vendor. While leveraging on the economies of scale and technical expertise of the supplier, the organisation needs to make sure that the outsourced IT project or service does not introduce security problems or vulnerabilities to the already-functioning internal systems, business processes and operations. This guide is an attempt to collate all security requirements relating to outsourcing, for which organisations...

Copyright SANS Institute
Author Retains Full Rights

AD

Automate more Web application scanning.
watchfire

A Security Guide For Acquiring Outsourced Service

GIAC GSEC Practical (v1.4b)
Bee Leng TIOW
19 Aug 2003

ABSTRACT

Outsourcing is not an abdication of the organisation's security responsibilities to an external contracting vendor. While leveraging on the economies of scale and technical expertise of the supplier, the organisation needs to make sure that the outsourced IT project or service does not introduce security problems or vulnerabilities to the already-functioning internal systems, business processes and operations.

This guide is an attempt to collate all security requirements relating to outsourcing, for which organisations seeking outsourcing should actively look into. It advocates the following activities be carried out by the organisations at various stages of outsourcing, in order to achieve a more holistic coverage of all security requirements and mitigating measures in outsourcing:

Pre-Outsourcing Activities

- Assess Security Risks
- Specify Security Requirements
- Assess Security Competency of Supplier

Outsourcing Activities

- Establish Contractual Obligations
- Assess Supplier Continual Performance

Post-Outsourcing Activity

- Post-outsourcing Security Requirements

It concludes by stating that outsourcing, like any other IT domains, is also not spared of security risks. For organisations adopting outsourcing to remain secure, it is important for them to understand their own outsourcing needs and the related risks, and to handle outsourcing in the right manner and in the correct context. With this, will it then be possible for the security risks of outsourcing to be effectively mitigated to an acceptable level.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

TABLE OF CONTENT

1 INTRODUCTION 1

2 SCOPE 2

3 ASSESS SECURITY RISKS 3

4 SPECIFY SECURITY REQUIREMENTS 4

4.1 SECURITY-RELATED SERVICE LEVEL REQUIREMENTS 4
4.2 PERSONNEL SECURITY REQUIREMENTS 4
4.3 SECURITY ROLES AND RESPONSIBILITIES 5
4.4 INFORMATION HANDLING AND DISCLOSURE 5
4.5 SECURITY TRAINING AND AWARENESS REQUIREMENTS 5
4.6 ACCESS CONTROL REQUIREMENTS 6
4.7 ACCOUNT MANAGEMENT AND ACCOUNTABILITY REQUIREMENTS 7
4.8 NETWORK SECURITY REQUIREMENTS 7
4.9 SECURE OPERATION REQUIREMENTS 8
4.10 AUDIT AND MONITORING REQUIREMENTS 9
4.11 INCIDENT MANAGEMENT REQUIREMENTS 9
4.12 OPERATIONAL CONTINUITY REQUIREMENTS 10

5 ASSESS SECURITY COMPETENCY OF SUPPLIER 11

5.1 SECURITY TRAINING AND AWARENESS 11
5.2 EXPERIENCE AND TECHNICAL EXPERTISE 11
5.3 EFFECTIVENESS OF SECURITY MEASURES 11
5.4 COMPLIANCE WITH ORGANISATION'S SECURITY POLICY, STANDARDS AND PROCEDURES 12
5.5 SUPPLIER'S SECURITY POLICY, STANDARDS AND PRACTICES 12

6 ESTABLISH CONTRACTUAL OBLIGATION 12

6.1 CONTRACTUAL OBLIGATIONS 12
6.2 LIABILITIES 13
6.3 RIGHT TO AUDIT 13
6.4 POST-CONTRACTUAL OBLIGATION 13

7 CONTINUAL ASSESSMENT OF SUPPLIER PERFORMANCE 13

8 POST-OUTSOURCING SECURITY REQUIREMENTS 14

8.1 REVOCATION OF USER ACCOUNTS AND ACCESS RIGHTS 14
8.2 DOCUMENTATION HANDLING 14
8.3 RETURN OF IT RESOURCES AND DATA 14
8.4 CONTRACTUAL OBLIGATIONS 14

9 CONCLUSION 15

REFERENCES 16

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

1 INTRODUCTION

Outsourcing -
The act of hiring an outside source, usually a consultant or application service provider, to transfer components or large segments of an organization's internal IT structure, staff, processes and applications for access via a virtual private network or an Internet-based browser.

Source: www.webopedia.com

Outsourcing is a business approach for organisations to relieve their IT budgets and resources to focus on more strategic business needs. For organisations that wish to tap on outsourcing, the benefits of outsourcing are certainly very attractive. It helps organisations save costs by leveraging on the economies of scale realised by the outsourcing suppliers. It also relieves the organisations from the problems of manpower constraints, skill shortages and operating inefficiencies.

In the IT industry, many services are available for outsourcing. Categorically, one can distil the characteristics of most outsourced services as being operational, routine or mundane in nature. That being so, it is important to recognise that the outsourced services are usually not those areas that organisations would like to build their core competencies in or have the capability to do so [1].

With this understanding, it is not difficult to see why outsourcing thrives in these IT domains:

- Facility management services[1]
- Managed Security services (MSS)
- Application development, implementation and maintenance (Also known as Application Service Provider, or ASP)
- Web site development, hosting and maintenance
- Email provisions and maintenance
- Database management services
- Business/disaster recovery services

Today, where competitive advantage is the key to survival and outsourcing of non-core business areas is a norm, the need has become greater for organisations to adopt a more secure yet methodical approach towards handling outsourcing. This will hence be the focus of this paper.

[1] Facilities management services can constitute such services as helpdesk support, software/hardware maintenance, software distribution support, asset management, server and network services, and so on.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

2 SCOPE

For this paper, the term "outsourcing" is to be understood as the transfer of ownership or responsibility of an IT function or service to an external organisation[2]. It is not the abdication of security responsibilities from the organisation to the supplier and the organisation must still be accountable for the overall security of the outsourced service. The outsourced service, in the context of this paper, refers to the IT project or service that is selected for outsourcing.

This paper is an attempt to advocate a generic list of security requirements that concerns the acquisition of an outsourced service from an external supplier. It will not be flavoured towards any specific type of outsourced service; neither will it cover how organisations should perform their business justifications for outsourcing or how organisations should integrate outsourcing with their IT procurement processes[3].

It is organised according to the processes below:

Pre-Outsourcing Activities[4]

- Assess Security Risks
- Specify Security Requirements
- Assess Security Competency of Supplier

Outsourcing Activities[5]

- Establish Contractual Obligations
- Assess Supplier Continual Performance

Post-Outsourcing Activity[6]

- Post-Outsourcing Security Requirements

[2] In outsourcing, the buying organisation does not instruct the supplier on how to carry out the task, rather it focuses on communicating what results it wants to achieve while leaving the process of accomplishing those results to the supplier.
[3] The National Institute of Standards and Technology (NIST) has produced a draft guide that discusses the security considerations for procurement of federal IT systems. The reference is provided at the end of this document.
[4] This refers to activities that the organisation should perform before an outsourcing contract has been established with the supplier.
[5] This refers to activities that the organisation should carry during the award of the outsourced service to a selected vendor and throughout the duration of the contract.
[6] This refers to the activity that the organisation is to perform upon the termination of an outsourcing contract.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

3 ASSESS SECURITY RISKS

While outsourcing relieves operational commitment on the part of the organisation, the act of engaging an external supplier to manage the IT service on its behalf may pose as security risks to the organisation [2]. Organisations should safeguard themselves against security risks such as:

- Unauthorised access to organisation's premise
- Unauthorised access to organisations' internal IT facilities and information (for connected services)
- Introduction of malicious codes (viruses, worms, trojan horses, trapdoors)
- Social engineering
- Attacks via service provider's systems/networks
- Non practice of due diligence on the part of service providers
- Inadequate operating processes or procedures

It is therefore necessary for the organisation to assess the security risks relating to outsourcing before proceeding to acquire the required service from a supplier. National Institute of Standards and Technology (NIST)'s *Risk Management Guide for Information Technology Systems* [3] is a good reference on how to conduct a proper risk assessment.

When performing a risk assessment, the organisation should take into consideration factors such as the purpose of outsourcing, scope of outsourcing, types and level of access needed by the supplier, duration, the strengths of protection offered by existing security controls put in place as well as the potential impacts to the organisation.

The derived outcomes from the risk assessment will aid the organisation and system owner in 2 ways:

i. Determining the level of risks and deciding if the level of risks is acceptable to the organisation
ii. Ascertaining the adequacy and effectiveness of security and procedural controls and whether additional mitigating controls are required

When the security risks are high, the business decision to outsource should be reconsidered. Outsourcing must not take place when the identified security risks cannot be effectively reduced or when security controls are assessed to be inadequate. Whenever possible, additional mitigating technical or procedural controls should be put in place to reduce the identified security risks to an acceptable level first.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

4 SPECIFY SECURITY REQUIREMENTS

When a decision is made on outsourcing, the organisation should proceed to list out the security requirements of the needed service. The security requirements must commensurate with the confidentiality, integrity and availability needs of the organisation as well as the outsourced service.

Covered below is a comprehensive but generic list of requirements. The organisation is advised to customise its own list of security requirements according to the nature and needs of the outsourced service.

4.1 Security-Related Service Level Requirements

4.1.1 Service Availability
The organisation should specify to the supplier the availability requirements of the outsourced service. This will be manifested in the form of a service level agreement, which should address such things as the scheduled operation time, performance level, downtime (be it scheduled or non-scheduled), availability measurement, and performance monitoring and error analysis.

4.1.2 Service Level for Reporting, Review and Resolution
The organisation should also define the supplier's service level for items listed below:

- Frequency of review of system and audit logs
- Turnaround time for reporting of security events such as incidents and violations
- Turnaround time for resolution of reported security problems
- Turnaround time for applying approved security patches, updates and changes
- Submission of reports such as periodic problem, audit and system reports

4.2 Personnel Security Requirements

4.2.1 Security Undertaking
The organisation should require all personnel assigned by the supplier to work on the outsourced service to observe the secure usage and handling of the organisation's information. The personnel should sign a letter of undertaking as agreement to these obligations. The liabilities for a breach of contractual agreement are also to be made known to the personnel at the start of the engagement.

4.2.2 Security Clearance
The organisation should require all supplier personnel who are working on sensitive or confidential projects (such as government projects) to be security cleared first before allowing them to work on the outsourced service. The

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

clearance requirements should comply with the security level determined by the system owner, the organisation and the relevant government authority.

4.3 Security Roles and Responsibilities

The security roles and responsibilities of all personnel involved in the outsourced service, whether from the organisation or the supplier, must be clearly defined and communicated. Clear definition of roles and responsibilities should not only ensure accountability and proper segregation of duty, but also prevent conflicting or duplicating roles from being defined.

4.4 Information Handling and Disclosure

4.4.1 Confidentiality Agreements

The organisation should require all personnel of the supplier who are to work on the outsourced service to sign a confidentiality agreement to protect the organisation against unauthorised disclosures of confidential information accessed by the personnel in the course of their work.

4.4.2 Proper Handling of Critical Information

The organisation should prescribe to all supplier personnel, who need to handle or are in custody of sensitive or confidential information, the appropriate manners to handle and manage these information. In this way, the organisation would be assured that its information is given the necessary protection.

4.4.3 Disclosure of Security Information[7]

The organisation should put in place a process or recourse for liability to protect itself against unauthorised disclosure of security information of the outsourced service, without the necessary approval or beyond the scope defined by the organisation. The disclosure of information by the supplier, if not properly managed, may create adverse impacts to the organisation.

4.5 Security Training and Awareness Requirements

4.5.1 Security Training and Competency

The organisation should require the supplier to assign the relevant skilled and experienced personnel to operate the outsourced service. The personnel should be familiar with the requirements of the outsourced service and the organisation, and should adhere to the security policy, standards and procedures stipulated by the organisation. The skill and experience of the assigned personnel should be verified by the organisation.

[7] Security information here refers to information pertaining to security incidents and breaches as well as critical security resources such as the operating systems, firewalls, intrusion detection systems and the like.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

4.5.2 Security Awareness in Work Area

The organisation should ensure that the assigned personnel of the outsourced service be fully aware of the security needs and risks in his/her assigned areas of work. This gives assurance to the organisation that these personnel will not, intentionally or unintentionally, compromise the security of the organisation or the outsourced service. The organisation should verify that the supplier has a comprehensive security programme to train its personnel in security and in their assigned role.

4.6 Access Control Requirements

This section will be relevant to the organisation if access to the premise or IT resources by the supplier personnel is needed. This type of access is commonly known as third-party access.

4.6.1 Assignment of Access Rights

As a general rule of thumb, any access to organisation's IT resources should be controlled and given only on a job need basis. The access should be approved by the system owner and tracked to ensure proper usage and accountability. Access control standards and procedures established by the organisation are to be followed closely.

4.6.2 Physical Access

The personnel should adhere to the physical access standards or procedure established by the organisation. If physical access to a restricted premise or IT resource is required by the personnel, a process should be put in place to verify that the access is properly justified and approved. The organisation should assign escorts to the supplier personnel, or to record/monitor all accesses made by the supplier personnel, in his/her visit to the premise or IT resource. All physical access should be terminated as soon as it is no longer required.

4.6.3 Logical Access

The organisation should put in place an approval process for the supplier personnel to acquire logical access to IT resources. Access to critical resources such as system files, logs and production data by supplier's personnel should not be allowed unless the access is properly justified and approved by the system owner. Access to these restricted resources should be tracked, monitored and reviewed regularly by the organisation to ensure that only authorised actions are carried out.

4.6.4 Remote Access

The organisation should not allow remote access by the supplier personnel as a default set up unless the access is properly justified and approved by the system owner. If applicable, the personnel should follow the remote access standards or procedure established by the organisation.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

The organisation should also ensure that the relevant security controls are implemented to protect the organisation against remote access related security risks like unauthorised access, loss of confidentiality and denial of service. Whenever possible, remote access should be given time-restriction and removed once the task is completed.

4.7 Account Management and Accountability Requirements

This section will be relevant to the organisation if user accounts are to be created in the organisation's IT system or network.

4.7.1 Designated User Account

Supplier personnel who are allowed access the IT resources and network should be given individual user accounts for authentication and accountability purposes. The organisation should discourage the sharing of user account so as to enable individual accountability. Access rights granted to the user accounts should be based on job needs, approved by the system owner and reviewed on a regular basis.

4.7.2 Logging

Logging mechanisms should be enabled on the user accounts held by supplier's personnel. The organisation should ensure that the logs are comprehensive enough. This will include the capturing of account, name, activities (both normal and exceptional activities), time, data and source of occurrence. If privileged accounts - like administrator, auditor, database administrator accounts - are also held by the supplier personnel then the logs should be set up to capture all activities carried out using these accounts. In addition, the organisation should make sure that a process is put in place for all necessary logs to be periodically reviewed.

4.8 Network Security Requirements

This section will be relevant to the organisation if access to the organisation network is given to supplier personnel.

4.8.1 Network Connectivity

If there is a business need for the supplier's network to be connected to the organisation's network, a review of the networks belonging to the supplier should be done. The review will help to verify that all external connectivity to the organisation's internal networks does not lead to compromise of the internal networks. The review should perform an assessment of the strength of the connectivity as well as to make sure that mitigating security controls have been put in place. The review process will give assurance to the organisation that any external connectivity will not become the conduit to attack the internal set ups of the organisation via the supplier's network.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

4.8.2 Non-trusted Network

Where it is not feasible for the organisation to perform a comprehensive review of the supplier's network connectivity, then the organisation should adopt the notion that all network connections external to it are not trusted. This notion is powerful because it will trigger the organisation to step up its efforts in implementing better mitigating controls to prevent its internal network from being attacked. When this happens, the organisation is encouraged to look into putting in additional controls such as additional firewall and intrusion detection system. The security policies, rules and signatures should be reviewed regularly to ensure that they remain current and relevant.

4.8.3 External Network Transmission

When external connectivity is permitted, the organisation should ensure that only authorised access-controlled network transmissions is allowed. Mechanisms like in-bound, out-bound traffic filtering, de-militarised zone and encryption are examples that organisation can put in place to limit security exposures.

4.9 Secure Operation Requirements

4.9.1 Secure Configuration

The organisation should ensure that the outsourced service is implemented and configured in a manner that supports the security level stipulated. Security configuration of critical IT resources, such as operating systems and firewalls, should be hardened and reviewed before the outsourced service becomes operational. This ensures that the outsourced service is not vulnerable to security exploits due to poor configuration practices.

4.9.2 Updates and Patches

Due diligence should be required of the supplier to perform the necessary patches and updates to the outsourced service, whenever the need arises. Updates and patches should be carried out in a timely manner. The organisation should be informed of the updates and patches to be performed.

4.9.3 Scanning

The organisation may require the supplier to perform periodic scanning for unauthorised codes and applications, viruses and system vulnerabilities, on the outsourced service. If any of the security weaknesses mentioned above has been found, the supplier is also required to perform follow-up actions to rid the outsourced service of these weaknesses in a timely manner.

4.9.4 Change Management

The organisation should define the types of change that are to be managed by it and by the supplier. Where it is required for the supplier to follow a change management procedure established by the organisation, the supplier's personnel should make sure that they adhere to it accordingly.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Hardware or software changes that are to be performed on critical IT resources such as system files, logs and application should be reviewed prior to implementation. The review should be performed by the system owner, together with the other relevant personnel. The change should be approved by the system owner and carried out after office hours to minimize disruptions to business operations.

4.10 Audit and Monitoring Requirements

4.10.1 Right to Audit

The organisation should establish the right to audit on the outsourced service and peripherals held at the supplier, whenever the need arises. The right to audit should also be extended to the supplier's subcontractors that are also involved in the service. The audit will allow the organisation to measure the security health of the outsourced service as well as to identify the existence of security weaknesses, if any. An independent auditor can be engaged to perform the audit.

4.10.2 Monitoring

The organisation should monitor activities by the supplier on the outsourced service on a periodic basis. The supplier is required to furnish the relevant reports and logs to facilitate the monitoring and reporting of activities carried out. Periodic monitoring helps the organisation to look out for anomalies in the outsourced service. Abnormal activities such as unauthorised changes to system and network files and directories should be quickly surfaced for investigation when detected.

4.10.3 Independent Review

An independent review should be performed on critical IT service that is outsourced. An independent reviewer, such as an external auditor, may be engaged to perform a security assessment on the IT service. In addition, in cases where it is not possible for the organisation to monitor the supplier's security compliance, the organisation could also consider the engagement of an independent reviewer to appraise the supplier's performance. For both situations, the independent reviewer should be reputable and competent in performing the review. The organisation should define the scope of review and require that the independent reviewer submit the review findings to it.

4.11 Incident Management Requirements

4.11.1 Incident Reporting

All security incidents that concern the outsourced service, such as viruses, security compromises, unauthorised access and modifications, and discovered security vulnerability, should be reported to the organisation. The supplier should be prevented from exploiting any vulnerability found in the outsourced service for its own gains or unauthorised purposes. A procedure

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

should be established between the supplier and the organisation to facilitate the reporting of security incidents. Whenever possible, the organisation's incident report procedure should be extended to the supplier. The personnel of the supplier should also be briefed and familiarised with the incident reporting procedure established.

4.11.2 Incident Handling and Response

The supplier should establish an incident handling and response capability. When a security incident takes place, the supplier should consult the organisation and work closely with the organisation's security personnel to handle and respond to the security incident. The supplier should also work closely with the organisation to implement preventive measures to thwart the recurrence of security incidents.

4.11.3 Alert Mechanisms

Alert mechanisms to notify on viruses, worms, vulnerability and exploits should be established between the supplier and the organisation. The organisation or the supplier should draw out and implement a security alert procedure. Personnel from the supplier should be familiar with the alert procedure and mechanisms established.

4.12 Operational Continuity Requirements

4.12.1 Backup and Recovery

The supplier should implement backup procedures and mechanisms to back up critical system files and government information stored in the outsourced service on a periodic basis. Back ups should be performed on reliable media, such as tapes, cartridges, CDs, and so on. Periodic checking should be performed to give assurance on the reliability of storage media that holds the information. In additional, secure storage such as offsite, should also be considered for safekeeping of critical files and data. Recovery procedures should be established by the supplier to ensure the availability and continuity of the outsourced service, as stipulated in the outsourcing contract.

4.12.2 Redundancies

Where availability of the outsourced service requires assurance, the organisation should require the supplier to implement redundancies into the outsourced service. Redundancies give assurance to the continuity of operations even when a component fails. Various forms of redundancies should be considered and implemented as deemed appropriate and business-viable. Examples include duplicate machines, network links, databases and so forth.

4.12.3 Business Continuity Plan

If the outsourced service is deemed as important for the organisation, then continuity of the service should be planned as part of the overall business continuity plan of the organisation. As with all business continuity plans, the

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

business continuity plan for the outsourced service should be reviewed, tested and updated to ensure business continuity effectiveness.

5 ASSESS SECURITY COMPETENCY OF SUPPLIER

This is an important practice to be performed by the organisation to get assurance about the supplier's ability, attitude and commitment to deliver, before the outsourced service is awarded. Manring advocated ten critical questions to ask potential service providers covering aspects such as having relevant track record, quality of supplier's infrastructure, charges and financial health [4].

This section will focus only on these aspects of assessing the supplier's competency:

- Supplier's personnel is security trained
- Supplier is experienced
- Supplier can comply with organisation's required security policy, standards and procedures
- Necessary security measures are put in place

5.1 Security Training and Awareness

The organisation should verify the presence of security training and awareness programmes for personnel of the supplier. This gives an indication to the organisation that the supplier personnel have been properly trained in security and will not become the weak links to the organisation subsequently. Usually, this is verified by interviewing the supplier, and checking the personnel credentials such as security certifications and training received.

5.2 Experience and Technical Expertise

The experience and technical expertise of the supplier's personnel should be verified to ensure that they are able to perform their work proficiently and competently. The organisation can interview the necessary personnel to assess their experience and skill levels. Another, perhaps the most effective, means is by speaking to the supplier's past references or present customers. Feedback from these two groups of customers is likely to give a more realistic indication as to whether the supplier is committed and able to deliver.

5.3 Effectiveness of Security Measures

The organisation should gain detailed understanding of the security mechanisms that the supplier deploys to protect its information and internal IT resources. This aspect is especially critical if the supplier is managing security-related outsourced service. In this case, it would be necessary for the organisation to make sure security measures like firewall, intrusion

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

detection system, logs, incident management, disaster recovery, etc., are properly handled by the supplier and effective throughout the contracting period. If possible, past audit reports should be acquired for verification or third-party security audit should be performed.

5.4 Compliance with Organisation's Security Policy, Standards And Procedures

In cases where the organisation's security policy, standards and procedures are to be followed, it would then be the responsibility of the supplier to make sure that the requirements are understood and followed. The organisation can specify these requirements either by communicating them to the supplier or by entering them into the outsourcing contract.

5.5 Supplier's Security Policy, Standards and Practices

Sometimes, depending on the nature of the outsourced service (for example, MSS), the supplier's security policies and practices may be required to be followed. In this case, the organisation will need to make sure that the supplier's policies and practices are adequate and that the organisation's IT systems will not experience a loss of confidentiality, integrity or availability. These are the three main issues related to security for IT service contract according to Carnegie Mellon University [5].

6 ESTABLISH CONTRACTUAL OBLIGATION

A contract is a legal document that states a formal agreement between two or more contracting parties. While it is used to establish understanding about the contracted service, it also legally binds the contracting parties to the terms and conditions specified. In adverse situations, the contract can be even be an instrument to facilitate enforcement and for seeking recourse.

In fulfilling the contractual requirements, the organisation should make sure that all contractual and security requirements are properly communicated to the supplier and its personnel. Where applicable, a copy of the contract and the organisation's security policies, standards and procedures should be extended to the supplier and personnel for compliance.

6.1 Contractual Obligations

The organisation should ensure that all security requirements to be complied by the supplier are explicitly entered into the contract with supplier [6]. The areas covered in section 4 are potentially the list of items that can be entered into the contract. Both *BS7799* and *COBIT's Audit Guidelines*, on the other hand, also provide their own list of items to be included in outsourcing contracts. [7, 8, 9]

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

The supplier, on this part, should be aware of the stipulated requirements for fulfilling its contractual obligations. Additionally, the supplier should also be made known the compensations and penalties that could be imposed by the organisation in the event of a non-compliance.

6.2 Liabilities

The conditions under which liabilities are to be sought from the supplier are to be clearly specified in the outsourcing contract. Usually liabilities in the form of compensation or penalty can be sought from the supplier if the supplier is found, either intentionally or negligently, to have caused a security breach, damage or injury. The liability requirements must be agreed and clearly understood by the supplier.

The advantage of stating liability requirements in outsourcing contract is that it not only discourages the suppliers from non-compliance of the mandatory security requirement stipulations or wrongdoings, it also allows the organisation to seek recourse when adverse events occur.

6.3 Right to Audit

The right to audit is an important mechanism for the organisation to gain assurance of the security health of the outsourced service. When the organisation enters this requirement into the outsourcing contract, it will give the organisation the right to exercise audit on the supplier, sometimes even on the supplier's subcontractors. If necessary, the organisation should also indicate the mode of the audit (say, by the organisation's internal audit department, by a third-party auditor or spot checks) and frequency required. The supplier should not only understand the rationale for audit but also provide all support necessary for the conduct of the audits.

6.4 Post-contractual Obligation

Post-contractual obligations by the supplier should be made known in the outsourcing contract. Some of these requirements pertain to the protection of confidential information and employment restriction of supplier or organisation staff. More of the post-contractual issues are discussed in section 8.

7 CONTINUAL ASSESSMENT OF SUPPLIER PERFORMANCE

Continual assessment and tracking of the supplier's performance gives assurance to the organisation that it is able to continue fulfilling its contractual obligations. In instances when the supplier's performance falls below the expectations or when the outsourcing practices deviate from the agreed plan, corrective actions can be taken immediately to bring the supplier back on track.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

The performance of the supplier should be continually assessed to ensure that it is able to fulfil its contractual obligations. Mechanisms should be identified to track the performance of the supplier. For instance, management reports and logs are means to validate the competency of the supplier on a continual basis.

The organisation should implement compensational mechanisms so that recourse can be sought when the supplier fails to perform in accordance to the contractual stipulations.

8 POST-OUTSOURCING SECURITY REQUIREMENTS

8.1 Revocation of User Accounts and Access Rights

All user accounts and access rights assigned to the supplier are to be revoked upon the termination of the outsourced service. The revocation should be carried out in a timely manner.

8.2 Documentation Handling

All information, documentation, equipment and assets of the outsourced service must be securely destroyed or returned, upon the termination of the IT outsourced service.

8.3 Return of IT Resources and Data

Where IT resources such as software, equipment, and sample data are handed to the supplier in the course of work, the organisation should ensure that such resources are returned as required. In cases where the supplier is requested to perform the deletion of given data previously used in the outsourced service, mechanisms such as reports or logs should be produced for the organisation to verify that proper data deletion had been securely and properly carried out.

8.4 Contractual Obligations

Should there be a need for the supplier to continue observing any of the contractual requirements, this should be made known to the supplier during the service termination. Examples of requirements where post-contractual obligations can be imposed on are the confidentiality of information and employment.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

9 CONCLUSION

Outsourcing is a double-edged sword. On one hand, it is a viable business option which yields economic benefits for organisations; on the other hand, it can be an avenue for security risks to be introduced into organisations if proper understanding and planning have not been reasonably afforded. As such, organisations adopting outsourcing as a business approach should achieve a balance of these two spectrums of needs.

This guide has attempted to provide a comprehensive list of security requirements and mitigating measures related to outsourcing. This is just the first step towards treating outsourcing securely. It may not be hard for one to notice that this guide discerns from any business context. This is intentionally because it is felt that each business environment is different and that describing one in this guide will not necessarily be helpful. In using the security requirements provided by this guide, it is essential also for the organisations to apply them in the correct business environments.

In conclusion, outsourcing like any other IT domains is also not spared of security risks. For organisations adopting outsourcing to remain secure, it is therefore important for them to understand their own outsourcing needs and the related security risks, and to handle outsourcing in the right manner and in the correct context. Only with this, will it then be possible for the security risks of outsourcing to be effectively mitigated to an acceptable level.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

REFERENCES

1. Corbett, Michael F., & Association, *Best Practices for Deciding What Should be Outsourced*, Firmbuilder.com, URL: http://www.firmbuilder.com/articles/5/27/518/

2. Harreld, Heather, *Outsourcing opens security risks*, Federal Computer Week, 5 Jan 1998, URL:http://www.fcw.com/fcw/articles/1998/fcw-risks-1-5-1998.asp

3. *Risk Management Guide for Information Technology Systems*, National Institute of Standards and Technology (NIST), Special Publication 800-30, Jan 2002, URL:http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

4. Manring, Audrey Y., *Ask Before You Outsource: Ten Critical Questions to Put to Potential Service* Providers, (i)Structure Inc., 2001, URL: http://www.coltexpress.com/files/WhyOutsource1_AskBefore.pdf

5. Security *for Information Technology Service Contracts*, Cert Coordination Center, Security Improvement Module, CMU/SEI-SIM-003, Jan 1998, pg 2, URL: http://www.cert.org/security-improvement/modules/m03.html

6. *CSI Roundtable on Outsourcing: managing related security* risks, Computer Security Institute, URL:http://users.bestweb.net/~bgeiger/art_paper/pr_csitable.htm

7. *Information security management, Part 1: Code of practice (BS7799-1:1999)*, sections 4.3.1 Security requirements in outsourcing contracts, British Standards Institute, 1999.

8. *Information security management, Part 2: Specification for information security management systems (BS7799-2:1999)*, sections 4.2.2 – 4.2.3, British Standards Institute, 1999.

9. *CoBIT Audit Guidelines*, CoBIT IT Steering Committee and IT Governance Institute™, CoBIT 3rd Edition, Delivery and Support 2.0, July 2000, pg 130.

10. Pankowska, M., *Outsourcing Impact on Security Issues*, University of Ecomomics, Information Systems Department, Katowice Poland, URL: http://figaro.ae.katowice.pl/~pank/secout2.htm.

11. Harris, Michael, *Inherent Security Risks in Outsourcing and Vendor/Partner connections – What the CIO Should Know*, Computer Security Journal, spring 1998, URL: http://www.secure20.com/pdfs/InherentSecurityRisksinOutsourcing.pdf

12. *Crafting a Better Outsourcing Contract*, White Paper, Everest Group, Inc., 1999, URL: http://nersp.nerdc.ufl.edu/~dicke/ism/everest.pdf

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

13. *Security Considerations in Federal Information Technology Procurements – A Guide for Procurement Initiators, Contracting Officers, and IT Security Officials*, National Institute of Standards and Technology (NIST), Draft Special Publication 800-4A, Oct 2002, URL: http://csrc.nist.gov/publications/drafts/800-4_PC_100802.pdf

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: September 5th, 2015

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Crystal City 2015	Crystal City, VAUS	Sep 08, 2015 - Sep 13, 2015	Live Event
SANS Network Security 2015	Las Vegas, NVUS	Sep 12, 2015 - Sep 21, 2015	Live Event
SANS Seoul 2015	Seoul, KR	Sep 14, 2015 - Sep 19, 2015	Live Event
SANS Tallinn 2015	Tallinn, EE	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Baltimore 2015	Baltimore, MDUS	Sep 21, 2015 - Sep 26, 2015	Live Event
Data Breach Investigation Summit & Training	Dallas, TXUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Perth 2015	Perth, AU	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS ICS Amsterdam 2015	Amsterdam, NL	Sep 22, 2015 - Sep 28, 2015	Live Event
SANS Bangalore 2015	Bangalore, IN	Sep 28, 2015 - Oct 17, 2015	Live Event
SANS Seattle 2015	Seattle, WAUS	Oct 05, 2015 - Oct 10, 2015	Live Event
SANS DFIR Prague 2015	Prague, CZ	Oct 05, 2015 - Oct 17, 2015	Live Event
SOS: SANS October Singapore 2015	Singapore, SG	Oct 12, 2015 - Oct 24, 2015	Live Event
SANS Tysons Corner 2015	Tysons Corner, VAUS	Oct 12, 2015 - Oct 17, 2015	Live Event
SANS Gulf Region 2015	Dubai, AE	Oct 17, 2015 - Oct 29, 2015	Live Event
SANS Tokyo Autumn 2015	Tokyo, JP	Oct 19, 2015 - Oct 31, 2015	Live Event
SANS Cyber Defense San Diego 2015	San Diego, CAUS	Oct 19, 2015 - Oct 24, 2015	Live Event
SANS Sydney 2015	Sydney, AU	Nov 09, 2015 - Nov 21, 2015	Live Event
SANS South Florida 2015	Fort Lauderdale, FLUS	Nov 09, 2015 - Nov 14, 2015	Live Event
SANS London 2015	London, GB	Nov 14, 2015 - Nov 23, 2015	Live Event
Pen Test Hackfest Summit & Training	Alexandria, VAUS	Nov 16, 2015 - Nov 23, 2015	Live Event
SANS Hyderabad 2015	Hyderabad, IN	Nov 24, 2015 - Dec 04, 2015	Live Event
SANS Cape Town 2015	Cape Town, ZA	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS San Francisco 2015	San Francisco, CAUS	Nov 30, 2015 - Dec 05, 2015	Live Event
Security Leadership Summit & Training	Dallas, TXUS	Dec 03, 2015 - Dec 10, 2015	Live Event
SANS Milan 2015	OnlineIT	Sep 07, 2015 - Sep 12, 2015	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced