Information Systems Outsourcing: Contract and Requirements for the Vendor

Jorma Kajava, University of Oulu, Department of Information Processing Science, Linnanmaa, FIN-90570 Oulu, FINLAND,
E-mail: jorma.kajava@oulu.fi

Paavo Jurvelin, Oulu Telephone Co., PL 30, FIN-90101 Oulu, FINLAND,
E-mail: paavo.jurvelin@mail.opoy.fi

Abstract

Outsourcing refers to the use of external companies to perform one or more organizational activities. It can be applied to a host of activities ranging from the use of contract programmers to managing third party facilities. The most common reason for companies to outsource their information systems include cost efficiency and the need to free resources for more essential functions.

As far as information security is concerned, the main considerations in outsourcing include laying down requirements for information security and drawing up the outsource contract, along with a number of security considerations during the actual outsourcing process and the at termination of the contract.

It is possible to reduce risks to information security in outsourcing by defining explicit information security requirements in the outsource contract. These requirements can be stated as a specific list of claims and standards. The contract should include an agreement of some specified period of time within which the requirements must be carried out. Threats to information security during the outsourcing process can be managed through supervision and revision. These measures must be taken into consideration in making the outsource agreement - the most important phase in the outsourcing process.

Keywords: outsourcing, information security, information security requirements.

1 Introduction

This work provides an overview of information security during the process of outsourcing. The purpose is to discover requirements for information security along with appropriate security control methods during the phases of the outsourcing process from the client's point of view. Aspects of information security in the outsourcing

process are viewed in chapter two. A concise definition of outsourcing is given and the phases of the outsourcing process are illustrated in the same chapter.

In this work, the term 'client' refers to an executive organization, who outsource their information system to a vendor, i.e. a service provider. In addition to stating requirements, this paper also examines aspects of information security in outsource contracts. This will be done in chapter three. The outsource contract is an important tool in convincing the parties involved that the level of information security provided by the vendor is high enough. Information security requirements for a service provider are described in chapter four. General requirements, report policy and supervision are essential elements for the client in maximizing security during outsourcing.

Economic aspects of outsourcing will not be examined in this work. Outsourcing will be limited to the client's information systems so, for instance, outsourcing software development will not be considered here. Furthermore, this paper does not attempt to describe detailed steps during the implementation of an information security programme or to provide implementation procedures for security controls.

2 Aspects of information security in outsourcing

2.1 Information security, outsourcing and insourcing

Information security is an abstract concept and it is therefore difficult to examine it as a real world object. However, complex real world issues can be illustrated by frameworks and models, and so can the concept of information security. Commonly accepted framework for information security is described by Donn B. Parker in his article "A New Framework for Information Security" [7]. According to Parker, information security means the preservation of confidentiality, integrity and availability of information from disclosure, modification and use by prevention, detection and recovery to reduce loss and risk of loss.

Outsourcing refers to the use of external agents to perform one or more organizational activities, such as purchasing goods or a service. It applies to everything from the use of contract programmers to management of third party facilities. This means that it is possible for an organization (client) to transfer its internal IS functions under the control of an outside company (vendor). Subcontracting differs from outsourcing in its scope as outsourcing involves a continuation of an existing IS, either partly or totally. Outsourcing can also be understood as a partial or complete transfer of responsibilities to a provider of outsourcing services [5].

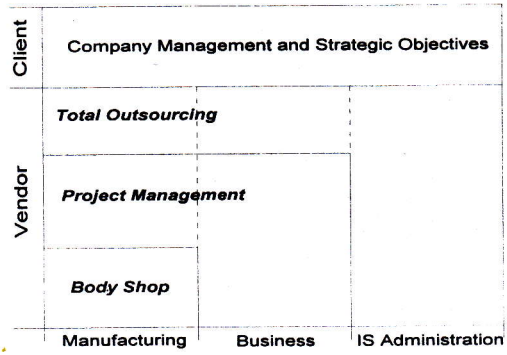

Figure 1. The ranges of IS outsource options

Insourcing, a relatively new term in IS management, constitutes the opposite concept to outsourcing. Basically, insourcing involves the partial or complete re-transfer of IS work back to the client organization. Outsourced IS work could be also moved to another provider of outsourcing services, but this is a matter of continued outsourcing and is not the same as insourcing.

2.2 The phases of the outsourcing process

During the preparation of outsourcing process, the client collects bids from various outsource vendors. In addition, the client should also evaluate the profitability of the vendors' bids [5]. During the next phase, the contract phase, the main task is to lay down the liabilities and obligations of the outsource parties, including security issues. Naturally, the scope and price of the outsourcing project must also be determined. The commencement phase, in turn, includes transferring the outsourced IS work into the facilities of the vendor; hiring and training the IS maintenance staff; and building up communications between the outsource partners. Then follows the actual outsourcing service, the external IS maintenance, which usually lasts a few years. After another evaluation is carried out, the outsource contract can be continued, in which case there may be some updates and changes in the contract. Drawing the outsource contract constitutes the most important phase of the outsourcing process. The outsource partners both want to increase their profits by the outsource arrangement.

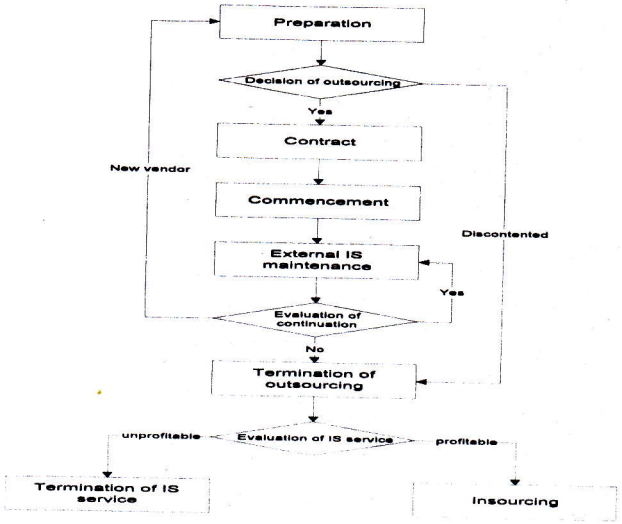

Figure 2. Information system outsourcing process.

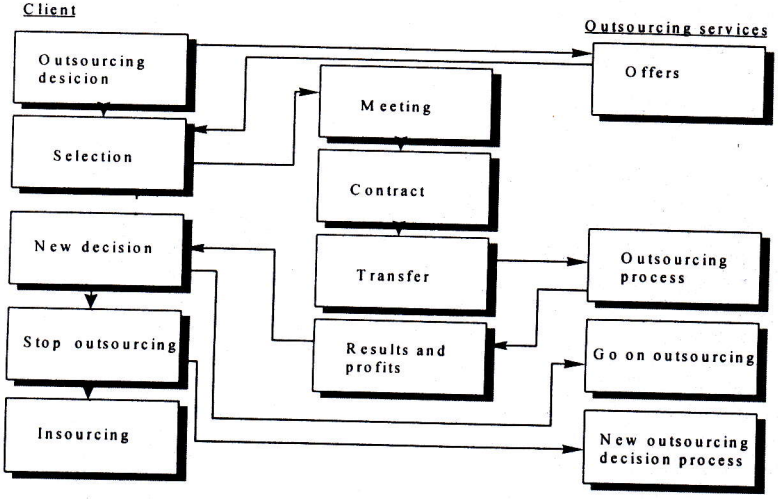

Figure 3. Flowchart describing the long-term outsourcing process with decision-making and actions.

2.3 Threats to information security during outsourcing

Numerous threats and security risks can be seen to be involved in the process of outsourcing. Thus, information security has to be at a high level to fulfill basic security needs and at the same time to protect the IS from threats associated with outsourcing.

Information security is achieved by the appropriate protection of confidentiality, integrity and availability of information. These basic aspects of information security are defined in the literature. Recently defined new elements of information security include the protection of the utility, authenticity and possession of information, presented by Donn B. Parker [7]. Particular threats to information systems regarding outsourcing include the following:

- the vendor may manage IS outsourcing facilities for the client's competitors
- disclosure or deletion of strategic and sensitive information
- the vendor may underestimate information security in outsourcing
- the partners could have conflicting goals in security management
- threats to information systems, personnel and data transfer
- the beginning and the termination of the outsourcing process
- insufficient methods of controlling and monitoring the vendor
- incomplete outsource contract

In total outsourcing, the client's main problem is the loss of direct control over the information systems [9]. The required level of information security in the outsourcing process must be defined in the outsource contract [3]. Drawing the contract constitutes the most essential phase of the outsourcing process, because it has a direct effect on the following phases. Consequently, explicit and unambiguous criteria for information security must be defined in the contract.

3 Information security concerns in the outsource contract

3.1 Concerns related to the management of information security

Information security should be managed throughout the phase known as IS maintenance. This management could take the form of supervision, report management and information security risk control. Risk management should be bilateral so that risks and threats to the information system can be identified, and appropriate security countermeasures implemented when deemed necessary. The vendor must have a tested and approved recovery plan for malfunctions. This is one way of ensuring service continuity. Concerns related to the management of information security in the contract should include clauses concerning supervision arrangements, liabilities and compensations, report proceedings in normal and exceptional situations, risk level control methods and the procedure for terminating the outsourcing process. Figure 4 presents a schematic representation of the management of information security during outsourcing.

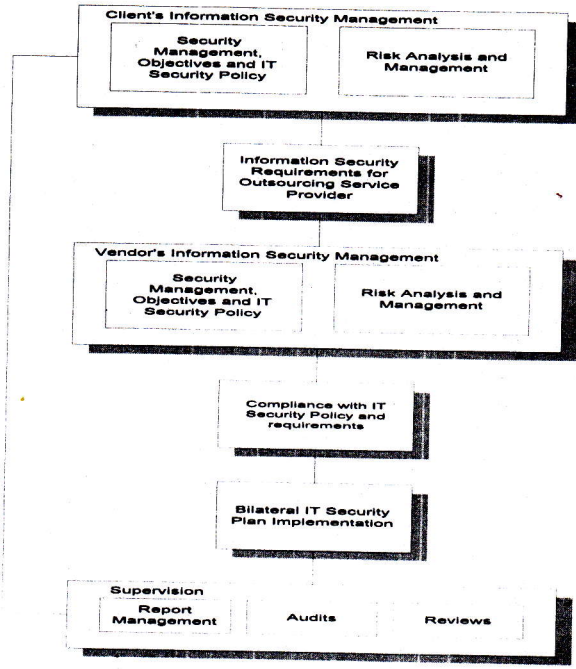

Figure 4. Management of information security in outsourcing.

3.1.1 Supervision, liabilities and compensations

The vendor bears the brunt of responsibility as far as security during IS maintenance is concerned. Therefore, terms regarding information security must be included in the contract and their implementation must be supervised. The vendor's responsibilities will be determined in accordance with the nature of the IS work in question. Supervision can be carried out by reports, audits, spot checks and inspection visits. The use of these arrangements must be agreed on in the contract.

The respective liabilities of the outsource partners must be defined, along with statutory regulations and commitments. These cover laws and regulations concerning data protection, patent, copyright and privacy. It would also be advisable to include clauses about trademarks, patents and copyrights in the contract [8]. Liabilities should include the assignment of responsibility in case of security incidents and disaster recovery. The persons who will be in charge of information security should also be stated explicitly [2]. There should be some special obligations in the contract regarding the vendor in case the vendor provides outsourcing services also for the client's competitors.

Compensation should be specified for cases where the vendor causes direct or indirect damage to the client. Furthermore, the contract should also specify the limitations in the vendor's liability and the restrictions on the total sum of financial compensation to be

paid to the client. The actual compensation procedure along with pecuniary penalties must be agreed on with the vendor and incorporated into the contract.

3.1.2 Reporting

Procedures, intervals, subjects and contents of reporting must be agreed on in the outsourcing contract. E-mail reporting should be avoided because of the security risks involved. If, however, electronic mail is used, all reports should be encrypted.

Normally, reporting involves information about system events and changes that are not urgent. These event reports should include the following subjects and they should be delivered regularly to the client.

1. Changes in security policy, responsibilities, personnel and system.
2. Suspected security and system weaknesses.
3. Security incidents.
4. IS events and present state.
5. System security testing results.

The vendor should have a logging systems concerning IS usage. These event logs make it possible to determine who, when and how the IT facilities are used. The logged events should also include errors such as the number of unsuccessful access attempts. Reports of these incidents should be enclosed in reports relating to exceptional situations. The client can also request that the vendor arranges logging in such manner that the users will be unable to modify - or even notice it [4]. The vendor should appoint a person to take charge of report management.

It is characteristic for exceptional situations that the point of time at which they occurred and the seriousness of the events are unknown. Nevertheless, they can be prepared for by adopting appropriate risk level control methods. The contents of reports relating to exceptional situations should include information of what happened, how long it took to recover from the incident and whether the vendor is able to get over the situation with no external help [4]. The question of what measures should be taken depends on the situation and can be agreed on immediately.

3.1.3 Risk level control methods

Regular reviews comprise the foundation of risk level control, which must be carried out during the IS maintenance phase. Results from the reviews are new measures which improve controls and safeguards. If there are major changes in the outsourced information system, risks to information must be reassessed to insure that security measures are updated with the progress of the information system. Information controls for all identified weaknesses must be implemented immediately. Technological progress brings with it new threats to information and may violate the integrity of information security. As new safeguards may still be in their swaddling bands and conflict with existing controls, one must be careful to ascertain that the new safeguards do not debase the existing information security controls [4][6].

3.2 The termination of the outsourcing process

After an evaluation including a profitability analysis, the client should decide whether or not to continue to use external IS services. If the client is discontented with the vendor's services, outsourcing can be continued with a new vendor. In this case, the IS will be transferred to the new vendor after careful preparation and the drafting of an agreement. Alternatively, the IS can be transferred back to the client's internal computing department or terminated permanently. The former option translates to insourcing the service. Although outsourcing is likely to extend over a long period of time, termination should be considered in the contract to avoid any future controversy.

The termination of outsourcing should be considered in the contract. The following aspects regarding information security should be taken into consideration in this context:

1. Transferring the IS back to the client.
2. Possible stoppages in the IS service during this transfer.
3. Returning all information assets back to the client.
4. Validity of the level of confidence after outsourcing.
5. Insourcing arrangements.

3.3 Identifying and establishing requirements for achieving information security

The client can ensure compliance with security policies and standards by means of a formal contract containing all the necessary security requirements. Finding out what those requirements are can be a daunting task. The nature of IS work offers a valuable starting point in this quest. Thus, the client should first determine the unique set of security risks and their potential consequences to his assets. In addition, the requirements should be outlined in accordance with the company's own security policy. It is important that the client's security policy supports the principles, objectives and requirements of information processing. The information requirements for the provider of an outsourcing service should be convergent with the implementation of security controls in the client's IT infrastructure [1].

The client should assess what influence outsourcing would have on existing information risks and IT security controls. Moreover, potential security risks must be taken into account during all phases of the outsourcing process. The client should apply common methods of risk assessment and analysis to identify threats and to estimate their potential consequences [6]. The results of this assessment should determine the appropriate security requirements depending, naturally, on the nature of the information system, the purpose for which the information is used, the environment in which the system is used, and the protection provided by the existing controls.

3.4 Stating requirements concerning information security

Generally accepted guidelines for information security can be used in stating information security requirements in the outsource contract. However, these guidelines can be of a too general nature for a specific line of business, in which case they must be

adapted to suit the situation. Generally accepted guidelines for information security are a worthwhile starting point in build up information security for a company.

The client can directly instruct the vendor in safety measures and methods or produce a specific list of requirements concerning the security of information, which is in fact the general recommendation, because general guidelines cannot necessarily be applied to a particular situation. One way of approaching the task is to draw up a list of requirements by improving and specifying general guidelines to meet the client's own particular needs. Moreover, a detailed list of requirements clarifies the principles underlying the security measures, and is thus a good way of avoiding any hassle during implementation. Furthermore, an extremely strict list of requirements can be a convenient way of reducing the number of vendor candidates. Some of the requirements, however, can be presented as alternatives and/or the partners can agree on a period of time within which the requirements must be fulfilled [4].

4 Information security requirements for the vendor

4.1 Organizational security

The vendor should be able to persuade the client that it has paid attention to issues related to information security in it's earlier business activities. The vendor should have a written information security policy, which the client can accept. This is one of the fundamental requirements associated with organizational security. Moreover, the vendor should handle issues related to information security in an organized manner. Furthermore, reciprocal information security can only be achieved if the security organizations of the outsource partners work in close cooperation, which also serves to assure the client that the vendor does not underestimate the security of information during outsourcing.

The unequivocal allocation of responsibilities concerning information security is of vital importance in protecting the client's assets. This is done to avoid any misunderstanding about reciprocal responsibilities. The client must assign a person to be in charge of these assets as well as other information security related processes. For instance, the client's IS maintenance staff must know the procedure in case of a security incident. They have to be aware of the reporting procedures and channels. Moreover, the protection of the client's assets also includes information assets. The vendor should report any replacements among personnel and changes in responsibility to the client. There must be explicit reporting procedures for both normal and exceptional situations.

The client should have mechanisms for controlling the service provider to ensure that security measures are followed. In addition, the client must have a right to audit contractual responsibilities. This could be carried out by periodic information security audits. All in all, the vendor's reporting obligation is a useful way of supervising IS maintenance and information security incidents.

4.2 Personnel

Information security should be taken into account at the recruitment stage and it should be included in job descriptions and contracts. Outsourcing complicates direct control of the outsourced information system personnel, so there will have to be mechanisms for ensuring the reliability of the staff, especially when the strategic value of the information is high. The vendor must check the backgrounds of the applicants and the client should be able to influence the allocation of duties. The client should be able to demand that an employee fulfills given qualifications for certain duties (e.g. academic degree). The employees should also sign a confidentiality agreement.

The outsource personnel must be trained in security matters and in the correct use of the IT facilities (e.g. computers and software). The use of equipment, service tasks and procedures must be documented, which will improve service continuity in case of replacements among personnel. Training in matters related with information security must be organized on a regular basis and the skills of the employees must be tested. Through education and meetings, the personnel should get a clear picture of their responsibilities regarding information security, including procedures for responding to security incidents. In addition, all employees must be aware of the reporting procedures.

The vendor must have reserve personnel for given tasks to improve continuity. The client should also consider the segregation of duties, such as the management and execution of certain duties (e.g. system administration and security audit), and thereby reduce opportunities for unauthorized use of data or services. The client should notify the vendor of disciplinary processes for dealing with employees who have violated the agreed-on security commitments.

4.3 Information assets

The vendor must have protection mechanisms for all forms of information. The information must be protected against modification, destruction, disclosure and misuse. The client can also determine a back-up policy for essential data and software. Back-ups should be regularly taken and stored in a remote location. They should also be regularly tested to ensure the reliability of their recovery.

The client should specify a classification for various kinds of information. Confidential material, in turn, can be assigned different levels of secrecy. Responsibilities can be addressed accordingly. The classification of information should cover labeling, distribution, users and usage, receiving and delivering, copying and filing, transportation, preservation and disposal.

4.4 Information security in data communication

The outsource partners should make an agreement on all data communication procedures, including electronic data interchange and data transmission by couriers. Data encryption should be considered for sensitive data. The client can request the use of a particular encryption algorithm to transform information into a cipher form. Furthermore, there should be an agreement on cipher-key management.

Message authentication techniques should also be considered for the transmission of sensitive data. Unauthorized changes and corruption of data must be detected. In addition to authenticating the sender of a message, authentication techniques can be used to ensure the integrity of the actual content of the message. For instance, the client can request the use of digital signatures to authenticate electronic data exchanges. These techniques should be applied to the use of electronic mail too.

The requirements for electronic and manual data exchange should be based on the sensitivity of the information. Information security issues should be considered and agreements made of the following subjects [1].

4.5 Physical and environmental security

As a basic security condition, the client can request that the vendor has appropriate alarm systems (e.g. fire, burglary) in the building. These alarm systems should be accepted by authorities (e.g. insurance company) and they must be checked periodically. The vendor must also have a locking system in the building and there should be physical entry controls to prevent unauthorized access to the IT facilities [4]. Physical entry controls should cover access policy for the vendor's personnel as well as visitors. In case of sensitive data, all activities in IS areas should be monitored and recorded. Extra requirements for unsupervised work should be considered to reduce opportunities for malicious activities. The client can also request that the vendor does not allow visitors in working areas, or that the visitors must at least be supervised and their access restricted.

4.6 Hardware and software

The vendor must comply with software licenses and regulations and prohibit the use of unauthorized software among the personnel, including software provided by the client. The client should only provide back-up versions of software for installation purposes.

The vendor must have up-to-date measures against computer viruses. Virus detection software must be regularly updated and used according to instructions. There could be automatic virus detection procedures, for example, during boot-up. Moreover, the client can request the imposition of special restrictions regarding the use of diskettes, such as prohibiting their use outside the actual working areas. Additionally, network file servers should also be taken into account in virus control. And finally, all virus related incidents should be reported to the client.

As for hardware security, only authorized access should be allowed to the site of the IT equipment. Smoking and eating should be prohibited in sensitive computer rooms. Hardware should be protected from power failures, and the equipment should be maintained according to hardware vendors' recommendations. In case of damage or aging, the equipment can be taken out of use. Before disposing of hardware, all data and software must be checked to verify the need of back-up copying. After back-up, all information and software must be deleted prior to disposal.

4.7 Operational security

Monitoring events in the working environment and monitoring data processing itself is part and parcel of operational security, as are, indeed, plans for ensuring the continuity of operation. This latter aspect can be improved by emergency and recovery planning. Continuity also can be improved by documenting all procedures for operating the IS. This also helps new employees to learn to use the IS faster, thereby minimizing the extent of interruptions. Breaks in operation caused by key-persons can be avoided by using trained substitutes. The outsource partners should have a clear agreement regarding the use of substitutes, however, trainees or temporary workers, for instance, should not be used in the outsourcing context.

Operational security can be improved by installing appropriate system access control methods. First of all, the vendor should have a documented access control policy, including user password management. Then, there should be user access profiles based on duties, legal access protection requirements and the client's own policies for information dissemination and entitlement. Moreover, all access attempts and certain service transactions should be logged so that they can be addressed to a single user without dispute. And finally, the vendor should have a person in charge of user accounts, whose user account report should be included in the main report [4]. The following subjects must be taken into account in achieving a basic level of operational security:

1. The accountability of the employees concerning all tasks and responsibilities should be implemented by defining user rights and transaction logging procedures.
2. The allocation of user accounts should be based on "need-to-use" principles included in job descriptions.
3. System access control methods should be used to prevent unauthorized access to IT facilities.
4. Password management should be rigorous.

Network access must be controlled including appropriate interfaces between the networked services, authentication mechanisms between the various network sites and methods of controlling user access to IT services.

5 Conclusion

As far as outsourcing is concerned, preparation is the most important phase in preventing threats to information. The essential task is to find a trustworthy vendor. Vendors can be made to compete with each other in terms of security matters, and their security policies can be reviewed and their backgrounds checked. During this phase, a final decision must be made whether or not to outsource. If the answer is yes, the next step involves drawing up and signing an outsource contract. The contract must contain clauses concerning the management of information security during outsourcing, requirements regarding particular control methods and actions the vendor must implement as well as certain contractual liabilities between the partners. These form the foundation of information security during the maintenance phase. Information security

can be carried out by means of appropriate risk level control methods, supervision and report management. Safety requirements can be discovered by applying risk management techniques to identify specific risks and threats related to outsourcing. In this respect, the nature of the information system is in a key position in this matter. The outsource partners have to adapt their information security practices to meet mutual standards. The termination of outsourcing must also be taken into account in the contract. During the termination phase, the main issues are the returning of the client's assets back to the client and the validity of confidentiality.

References

[1] A Code of Practice for Information Security Management. 1993. Department of Trade and Industry. GBIS. PD 0003, London, UK.

[2] Fried, L. 1993, Distributed Information Security. Information Systems Management. Vol. 10, Iss. 3, 56 - 65.

[3] Kajava, J., Viiru, T. 1996. Delineation of Responsibilities regarding Information Security during an Outsourcing Process from the Client's Point of View, IFIP TC 11, Sec'96/WG11.1,Pythagorion, Greece.

[4] Kajava, J., Jurvelin, P., 1996. Outsourcing as a Business Option in Secure IT Environment. University of Oulu, Department of Information Processing Science, Working Papers Series B 45, Oulu, September.

[5] Lacity, M. C. & Hirschheim, R. 1993. Information Systems Outsourcing - Myths, Metaphors and Realities. Guilford, Surrey: John Wiley & Sons.

[6] Miettinen, J. E. & Kajava, J. 1994. Risk analysis and risk assessment - an overview of basic ideas and commonly used techniques, (in Finnish). University of Oulu, Department of Information Processing Science, Research Papers Series A20.

[7] Parker, D. B. 1995. A New Framework for Information Security to Avoid Information Anarchy. In Eloff J. H. P. & von Solms S. H. (eds.) Information Security - the Next Decade. London: Chapman & Hall, 155 - 164.

[8] Wildish, N. 1993. Outsourcing IT - Safeguarding Your Legal Interests, Purchasing & Supply Management, December 1993, 30 - 33.

[9] Wong, K. 1993. How to Implement an End-to-End Security Framework. Computer Fraud & Security Bulletin.