IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 12, Issue 3 (Jul. - Aug. 2013), PP 96-102
www.iosrjournals.org

Information Security Management System: Emerging Issues and Prospect

Amarachi A.A[1], Okolie S.O[2] Ajaegbu C[3].
Computer Science Dept, Babcock University,Nigeria
Computer Science Dept, Babcock University,Nigeria
Computer Science Dept, Babcock University,Nigeria

***Abstract*: *Information Security Management System (ISMS) can be defined as a collection of policies concerned with Information Technology (IT) related risks or Information Security Management (ISM). Majority of ISMS frameworks that have been implemented and adopted by organizations, centre on the use of technology as a medium for securing information systems. However, information security needs to become an organisation-wide and strategic issue, taking it out of the IT domain and aligning it with the corporate governance approach. The aim of this paper is to highlight the available ISMS frameworks, the basic concept of ISMS, the impact of ISMS on computer networks and internet, the chronological developement of ISMS frameworks and IT Security Management/IT Security Organization. These were accomplished through the review of existing literatures on ISMS frameworks. In essence, it was observed that there is need for every organisation to have an information security management system that can adequately provide reasonable assurance and support for IT applications and business processes*.

Submitted date 20 June 2013 **Accepted Date: 25 June 2013**

I. Introduction

A management system describes the processes, technologies and people used to emphasize and manage the activities of an organization. Each organization builds a unique system that supports the goals of that organization. The system will reflect different disciplines depending on the values and culture of the organization. So, we see systems defined with very different areas of focus such as health, safety, quality, enterprise management, environment, web content, personnel, risk and many other topics; and with different emphasis on security factors such as confidentiality, integrity, availability, or on topics such as privacy or product assurance.

Information Security Management System (ISMS) is a documented system that provides security for information and data in an organization. Every organization is faced with the task of providing a comprehensive plan for information security. Caralli & Wilson (2004), opined that "modern organizations have a huge challenge on their hands as they must secure the organization in the face of increasing complexity, uncertainty, and interconnection brought about by an unprecedented reliance on technology vis-à-vis legislative policies on security".

Today's information systems are complex collections of technology (i.e., hardware, software, and firmware), processes, and people, working together to provide organizations with the capability to process, store, and transmit information in a timely manner to support various missions and business functions. Information needs to be available, accurate and up-to-date to enable an organization make good business decisions. While various ISMS frameworks have been implemented and adopted by organizations, the focus has been more on the use of technology as a means of securing information systems. However, information security needs to become an organisation-wide and strategic issue, taking it out of the information technology (IT) domain and aligning it with the corporate governance approach. Furthermore, an algorithm-based ISMS model demonstrating ITGC concepts, is proposed with a more human-centred approach, in order to achieve a more efficient guide to information security management.

Despite the fact that each organization builds a unique system, the management systems have several common elements, and are based around an improvement cycle. One frequently used is the popular "Plan-Do-Check-Act" (PDCA) cycle lectured in Japan (Deming, 1950). This cycle is used as a guide in planning the action of what needs to be done and how best to go about it, establish the controls needed, monitor progression, and improve the system - taking preventive and corrective actions and pointing out areas for improvement. The analysis of management systems has shown that there are various common elements including policy, planning, implementation and operation, performance assessment, improvement, and management review.

This paper will present a near exhaustive review of management systems for information security using resources provided by various researchers in the field of ISMS. It will also provide an introductory motivation; showing where security risks arise and how they can be managed in organizations.

II. Basic Concepts Of Isms

An Information Security Management System (ISMS) can be defined as a collection of policies concerned with Information Technology (IT) related risks or Information Security Management (ISM). The phrasal idioms arose primarily out of ISO 27001, which is the standard used to scrutinize the security framework and thus ensures a functional solution is created. The ISMS must have access into all systems and information in organizations. Without strong security controls, businesses risk the possibility of financial loss, legal liability, and reputation harm. The insecurity of the Internet further exposes institutions to undetected, global, and virtually instantaneous attacks on internal systems and proprietary information. See fig 1

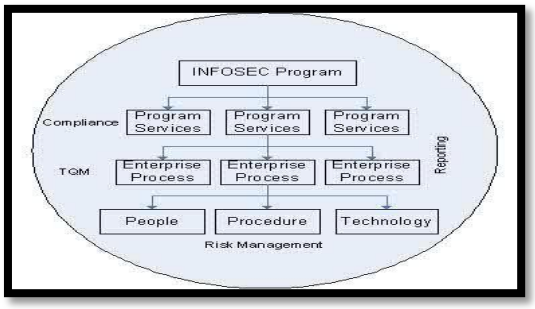

Figure 1: The Concept Of ISMS
Source: Carlson, T. (2008). Understanding Information Security Management Systems. New York: Auerbach Publications.

All employees, whether in the private or public organizations possess information. Most of this information exists in many forms, and different types of information have different values to an organization. With a wide range of information threats organizations face, it is important to enforce ISMS which Brykczynski & Small (2003), opined that "the life-cycle approach to implement, maintain, and improve the interrelated set of policies, controls, and procedures that ensure the security of an organization's information assets need to be in a manner appropriate for its strategic objectives".

With the ever-increasing number of people connecting to the Internet, security has become increasingly more important. "The number of computers connected to the Internet is still increasing dramatically from roughly ninety-seven million in the year 2000 to more than one hundred and thirty-seven million in the year 2001" (Parenty, 2003). As much as web services offer many benefits, its new advancements also pose many new threats to ISMS. Security systems used by organizations presently include: firewalls, virus protection programs, encryption, etc., while the future systems will need new Extensible Markup Language (XML) standard formats like XML Encryption, XML Digital Signature, XML Key Management Systems to structure the security data . Although XML solves some problems, it has also created security questions that need to be answered. The chief objective of ISMS is to implement the appropriate measurements in order to eliminate or minimize the impact that various security related threats and vulnerabilities might have on an organization. By so doing, Information Security Management will enable implementing the desirable qualitative characteristics of the services (such as; availability of services, preservation of data confidentiality and integrity) offered by the organization.

any steps are involved in building an ISMS. While performing each step, inputs from all stakeholders in the organization should be included and results discussed to reach an agreed upon path. A security manual serves as the central repository for ISMS. This manual, usually considered a confidential document, will be maintained by the Chief Security Officer. The various steps involved in building an ISMS are:

i. **Step1 - Risk Assessment:** An organization-accepted security risk assessment should be done. The goal is to identify assets, threats, vulnerabilities and controls to mitigate risks. Some risks will be accepted and management approval should be attained on this.
ii. **Step 2 - Top-down approach:** Security is a management issue and not just an IT issue. Hence it is critical that top management plays an important role in building an ISMS. Management should have the overall ownership of ISMS. Management should encourage a culture within the enterprise to follow security principles.
iii. **Step 3 - Functional roles:** Once the management's approval is attained, functional roles will have to be identified. Depending on the type and size of the enterprise, the roles can vary in type and number. A chief information security officer should be identified who solely owns the ISMS. Other functional roles could include Data stewards, Security awareness trainers etc.

iv. **Step 4 - Write the policy:** The security policy is a document that states the organization's information security strategy at a high level. The language in the policy is derived from the risk assessment. Details should be avoided in a policy. In order to make the policy acceptable to all stakeholders, the manner in which the policy is expressed should be at a high level and align nicely with the organization's business priorities and goals.

v. **Step 5 - Write the standards:** Standards are definite requirements that an organization should put forth for everybody to follow. The standards should support the security policy and be measurable. It is good practice to document what the penalties are when standards are not met.

vi. **Step 6 - Write the guidelines and procedures:** Guidelines are recommended ideas for an organization. They can also be termed as 'nice to haves'. It should be noted that the effectiveness of an organization's security management will not be measured by the guidelines present. There, usually, are no penalties for not following the guidelines. However, there can be some incentives if the organization follows the guidelines. Procedures are step by step description on how to meet the standards or guidelines so that the policy is supported. Procedures are usually targeted at the system level people who actually implement the control.

According to National Institute of Standards and Technology (NIST) Computer Security Division (2010), "today's participants of ISMS include complex assemblages of technology (i.e., hardware, software, and firmware), processes, and people, working together to provide organizations with the capability to process, store, and transmit information in a timely manner to support various missions and business functions" as shown in Figure 2 .

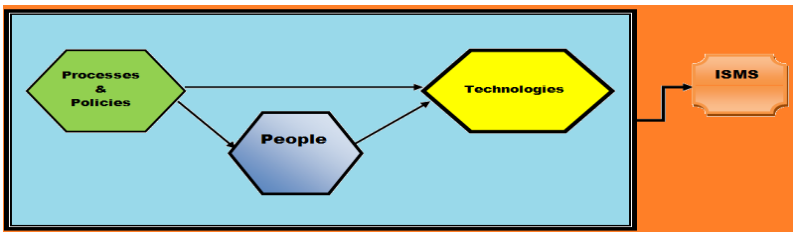

Figure 2: Isms Participants

III. Review

Pattinson (2007) noted that "an information security management system (ISMS) focuses on managing information security within an organization, a subject that is of developing concern to many organizations as they deal with the challenges presented in the information society. These challenges include: evolving information security and privacy legislation, published guidelines (Organization for Economic Co-operation and Development (OECD), Cyber security), and natural threats (fire, flood, earthquake, tornados) or human threats (viruses, spam, privacy, hacking, industrial espionage)". In Information Security Management Systems (ISMS), the information protected goes beyond that residing in electronic formats on computers or networks, but includes paper-based information and extends to intellectual property.

Peltier (2005) provided key qualitative insights with a systems approach toward the humanistic side of information security. The research firmly presents two realms of information security: one lies in the humanistic communication of individuals and the other in information transactions over the computer (virtual). Peltier urges that an effective information security program cannot be implemented without the implementation of an employee awareness and training program that addresses the policy, procedures, and tools, so that each individual may understand and utilize.

Pattinson (2007) has written a paper to thoroughly investigate the pith of ISMS. He notes thus, "by using an ISMS an organization can be sure that they are measuring and managing their information security processes in a structured manner and that they can control and hone their system to meet their business needs". If they draw from a standardized ISMS framework they can be sure that they are drawing from the experience of many others and that the system has been reviewed and reflects best practices. Such a framework is a tried and tested tool that helps management ensure that security-resource is spent on the most effective areas for the business (Pattinson, 2007).

Carlson (2008) characterizes information security management systems as "coordinated activities to direct and control the preservation of confidentiality, integrity, and availability of information". He notes the concept of ISMS thus: "ISMS is an example of applying the management system conceptual model to the discipline of Information Security". Unique attributes of this instance of a management system include:

a. Risk management applied to information and based upon metrics of confidentiality, integrity, and availability
b. Total Quality Management (TQM) applied to information security processes and based upon metrics of efficiency and effectiveness.

c. A monitoring and reporting model based upon abstraction layers that filter and aggregate operational details for management presentation.
d. A structured approach towards integrating people, process, and technology to furnish enterprise information security services.
e. An extensible framework from which to manage information security compliance.

ENISA (2010) notes that the chief target of Information Security Management is to implement the appropriate measurements in order to eliminate or minimize the impact that various security related threats and vulnerabilities might have on an organization. In doing so, Information Security Management will enable implementing the desirable qualitative characteristics of the services offered by the organization (i.e. availability of services, preservation of data confidentiality and integrity etc.). The framework of ISMS is illustrated in *Figure 3.*

The ENISA agency further explains that small businesses with limited information systems infrastructure, whose operation do not demand handling, storage and processing of personal or confidential data, usually face minor risks or risks with lower likelihood or impact. These organizations are more likely not to maintain independent ISMS and usually deal with information security risks ad-hoc or as part of a wider Risk Management process. Larger businesses and organizations such as banks and financial institutions, telecommunication operators, hospital and health institutes and public or governmental bodies have many reasons for addressing information security very seriously. Legal and regulatory requirements which aim at protecting sensitive or personal data as well as general public security requirements impel them to devote the utmost attention and priority to information security risks.

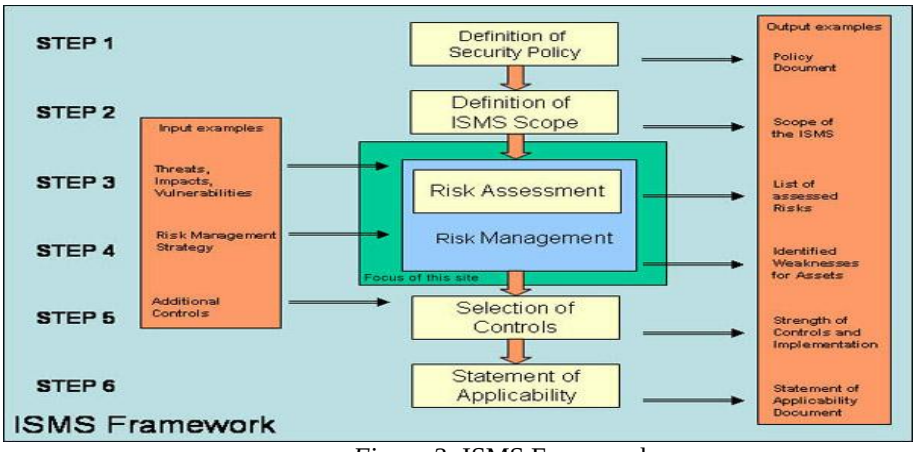

Figure 3: ISMS Framework

Source: European Network and Information Security Agency (ENISA). (2010). ISMS Framework.

A properly implemented ISMS can be effectively used by either small or large organizations, and can be tailored to support the protection of information in diverse organizations including data processing centers, software development, e-commerce, health care organizations, finance, manufacturing, service organizations, non-governmental organizations, colleges, and not-for-profit organizations.

Effective implementation of an ISMS framework ensures that a management team, committed to information security, provides appropriate resources to support the processes that the organization needs, in order to achieve appropriate information security. It needs to be stressed that this commitment of senior management is of extreme importance in the success of this - and other - management systems.

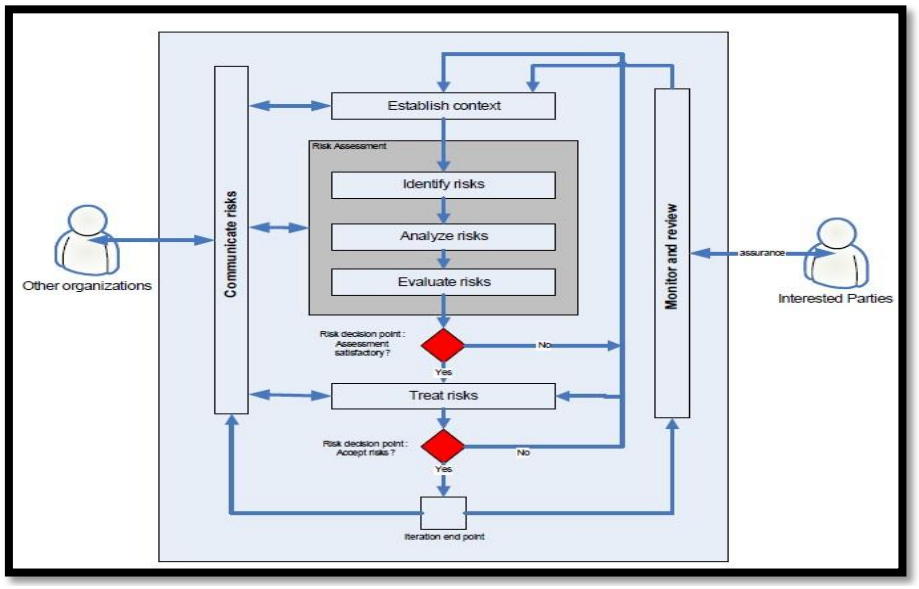

Figure 4: The Risk Management Process
Source: Pattinson, F. (2007). *Certifying Information Security Management Systems.*

This inevitably includes processes related to the basic management of the system, training and awareness. It emphasizes a risk management process (see fig 4) that guides the choice of safeguards and that, coupled with the metrics necessary to ensure that the chosen controls are implemented correctly, ensures that the system evolves to manage the changing business and security environment, and that the resulting management system is, and continues to be, effective.

IV. Impact Of Networks And The Internet On ISMS

Before computers, information was kept mainly as paper records, accessible only by a few authorized individuals. As the use of computers and networks grew, more and more of this information began to be stored electronically. This allowed a large number of people access to information enabling the improvement of the organization's value. It also allowed many unauthorized people access to this information for their personal use. Finding ways to safeguard this information in such a way that policies, processes and people are invloved, became an important mission, and continues to be so today.

Networks and the Internet made it possible for companies to send information to almost anyone, anywhere and at anytime. However individuals who wanted to use this confidential information for their own personal purpose could now access this information. These individuals are commonly referred to as crackers. Crackers can easily obtain this information by tapping into organization networks through the Internet and impersonating authorized users. Once crackers have the private information of consumers, they can use it to pursue their own personal interests. One such way in which crackers use this information is identity theft, in which a person pretends to be another person in order to obtain credit cards and make unauthorized purchases, among other things. With crackers came the need for better computer security. Security now needed to span time and space to keep confidential information out of the hands of malicious users.

With the emergence of computers and the popularity of using the Internet, security has become its own business. There are many people who specialize in Internet security. Viruses have also exploded onto the scene. Over one thousand three hundred new macro viruses were detected in 1997 compared with about forty in 1996 (Burgess, 2002). Eight years ago the number of macro viruses grew to about one thousand two hundred and sixty. One main security system used by companies is the firewall. A firewall controls the information that passes between an organization's computers and the Internet. (Parenty, 2003) states that "a firewall can adopt one of two basic policies to control access from the Internet to an internal computer". The first is whatever is not prohibited is allowed and the second is whatever is not allowed is prohibited". The main protection that the firewall does not provide is protection against attacks that originate from within the organization.

Prior information has shown us that at times information systems design were often developed with lack of foresight, and that unknowingly allows systems to become more vulnerable (Ghosh, 2004). For example, Web services offer so many immediate benefits; information technology departments often implement these programs without considering security issues. It is not until later; when a security breach occurs that steps are taken to secure their vital information. The advancement of Web services alone poses many new threats to information systems.

V. Chronological Developement Of ISMS Standards

In the area of information security, various standards have been developed in which emphasis is placed, in part, on other target groups or subject areas. The use of security standards in organizations or government agencies not only improves the level of security, their use also makes it easier for organizations to agree on which security safeguards must be implemented in what form (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2009).

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee for creating and publishing ISMS standards. An ISMS standard called IEC:ISO17799 was founded in 1987 as British Standard 7799 part 1 by the Department of Trade Industry (DTI). As a result of its efficacy, there was growing interest to adopt the standard in many other countries worldwide.

VI. IT Security Management And IT Security Organization

There are many standards, models and framework for information security management. Among the first standards is called the BS7799 that was released in 1999. A paper has been written by Li. et al. (2003) to present the BS7799 standard. They have presented this standard as a suitable model for information security. The BS7799 is based on a standard archived by best practices in the information security management area. Organizations have been using their own developed frameworks earlier. They have concluded that BS7799 together with organization-specific requirements, is the most effective way of providing information security.

In the paper information security management standard: problems and solutions written by Siponen (2003), there have been critical analyses of the three widely used information security standards in 2003 and earlier. The conclusion of this paper boils down to the fact that these normative standards are claimed to be generally valid and not based on what is done in other organizations like in research approaches.

An extensive survey carried out by Stamland (2004) checks if BS7799 is worth the effort. He concluded that organizations certified according to BS 7799-2 have higher maturity than organizations that have chosen to only use the standard in an informal way. Those organizations that use the standard informally have higher maturity than those organizations that do not implement any ISMS. He believes that the findings support the statement. BS 7799 will be worth the effort for organizations which need to protect their assets.

Solms (2005) has written a paper to investigate the co-existence and complementary use of Control Objectives for Information and related Technology (COBIT) and ISO 17799 as reference frameworks for Information Security governance. The investigation is based on a mapping between COBIT and ISO 17799 and provides a level of 'synchronization' between these two frameworks. He has presented COBIT as 'the tool for information technology governance'. COBIT is therefore not exclusive to information security. It addresses Information Technology governance, and refers amongst many other issues, to information security. The downside of using COBIT for Information Security governance is that it is not always very detailed in terms of 'how' to do certain things. ISO 17799 is exclusive to information security, and only addresses that issue. The upside of using ISO 17799 for Information Security governance is that it is more detailed than COBIT, and provides much more guidance on precisely 'how' things must be done. The downside of using ISO for information security is that it is very much like "stand alone" guidance, not integrated into a wider framework for Information Technology governance. His suggestion is to use a mapping of the standards so it takes the best from both standards by making the very useful content provided by COBIT and ISO 17799, much more useful in implementing comprehensive and standardized Information Security governance environments.

Making sense of information systems security standards has been presented by Tejay (2005). This paper concludes that there are a plethora of standards and it is not effective and economical to adopt these to organizations. A set of security standards working coherently as an integrated model and aligned with its business objectives is suggested. The set would integrate a minimum set of standards to cover maximum IS security needs of an organization.

An approach for internal auditors and IS Managers to establish the extent to which their organization complies with the international standard AS/NZS 17799 (IEC:ISO 17799) is proposed by Pattinson (2003). This approach incorporates a set of baseline IS controls, extracted from the standard, with a Goal Attainment Scaling (GAS)-based evaluation methodology.

Some researchers have recognized that relationship between security objectives and practices are complicated, but important for practitioners to understand. Pearson and Ma (2005) have done a survey about objectives and practices in information security management by a canonical analysis based on data from three

hundred and fifty-four security professionals. In the survey they have found that "Confidentiality" is the highest correlation with information security practices. They concluded that it is important that practitioners must take an appropriate management intervention to improve the effectiveness of information security management.

VII. Conclusion

Studies have shown that there is need for every organisation/industry to accomodate the use of an information security management system in its operation. The currently existing frameworks for this system have centered much on the use of technology as a means of securing information systems. There is need for information security to become widespread so much so that strategic issues be expunged from the IT domain and aligned with corporate governance approach. This paper took a look at the available works on ISMS and had identified how ISMS can be developed not only to offer security but also to enhance corporate governance. The proposed framework for this will be shown in part II of this paper.

References

[1] Brykczynski B. & Small B. (2003). Securing Your Organization's Information Assests (p. 1). Retrieved from 10.1.1.177.8675.pdf
[2] Bundesamt für Sicherheit in der Informationstechnik (BSI). (2009). BSI Standard 100-1 – Information Security Management Systems (ISMS)
[3] Burgess, S. (2002). Managing Information Technology in Small Business: Challenges & Solutions. Victoria University, Australia. Idea Group Publishing.
[4] Caralli, R. A. & Wilson, W. R. (2004). The Challenges of Security Management (p. 1). Retrieved from ESM White Paper v1.0 Final-2.doc
[5] Carlson, T. (2008). Understanding Information Security Management Systems. New York: Auerbach Publications.
[6] Deming, E. W. (1950). Evolution of the "Plan-Do-Check-Act" (PDCA) cycle. JUSE.
[7] Department of Trade and Industry (DTI). (2006). Information Security. Retrieved from http://www.dti.gov.uk/industries/information_security
[8] European Network and Information Security Agency (ENISA). (2010). ISMS Framework. Retrieved from http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/rm-isms/framework Ghosh, S. (2004). The Nature of Cyber-attacks in the Future: A Position Paper. Information Systems Security (p.18), 16p.
[9] Li et. al, (2003). BS7799: A Suitable Modell for Information Security Management.
[10] Parenty, T. (2003). Digital Defense. Boston, Massachusetts: Harvard Business School Press.
[11] Pattinson, F. (2007). Certifying Information Security Management Systems. Retrieved from http://www.atsec.com/downloads/pdf/CertifyingISMS.pdf Pattinson, M. R. (2003). Americas Conference on Information Systems.
[12] Peltier, T. R. (2005). Information Security Policies, Procedures and Standards, Guidelines for Effective Information Security Management (pp. 1-3), Boca Raton, FL: CRC Press.
[13] National Institute of Standards and Technology (NIST) Computer Security Division (2010) Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. Information Management & Computer Security, 8 (1), 31-41.
[14] Stamland, F.A.(2004). Is BS7799 worth the effort.
[15] Tejay, G. (2005). Making Sense of Information Systems Security Standards, Americas conference on Information Systems.
[16] von Solms, B. (2005). Information Security governance: COBIT or ISO 17799 or both? Computers & Security, 24 (2), 99-104.