NEW INFORMATION SECURITY ARCHITECTURE

T Grobler

Prof B Louwrens

University of Johannesburg, Department of Business IT

talania@twr.ac.za

University of Johannesburg, Academy for Information Technology

BuksL@nedcor.co.za

ABSTRACT

Information security has become an essential part of our daily lives. Organizations have accepted that the protection of the information and information assets is a fundamental business requirement. Managers are implementing an increasing number of security counter measures, such as security policies, intrusion detection systems, access control mechanisms and anti-virus products to protect the information and information assets from potential threats.

The management of Information Security is becoming problematic in industry, as companies do not follow an integrated, holistic management approach. Many security professionals and managers find it difficult to obtain a comprehensive understanding of their organization's security posture. Limited budgets and staff prevent security professionals to handle the security demands properly. Managers must be able to assess the security posture of an organization to determine the effectiveness and efficiency of the security implemented in the organization.

However, when a security incident has taken place, many organizations do not have proper guidelines to conduct a forensic investigation and often fail to bring the investigation to a productive conclusion. Many organizations do not regard forensic investigations as a priority item (Sinangin, 2002). A digital forensic management model (DFMM) is necessary for successful investigations.

The aim of this paper will be to use elements of existing information security architectures and propose a new architecture. The new architecture will be based on various dimensions of Information Security and can be used as a framework to manage, implement and assess the security posture of an organization. This paper will also pose the question whether the DFMM should be part of the Information Security Architecture.

KEYWORDS:

Information Security, Information Security Management, Information Security Architecture, Security Dimensions, Digital Forensics

1 INTRODUCTION

Information Security can be defined as the process of protecting information and information assets from a wide range of threats in order to ensure business continuity, minimize business damage, maximize return on investments and business opportunities by preserving confidentiality, integrity and availability of information (ISO17799, 2004).

Information Security is a multi-dimensional discipline. Some of the dimensions identified by Von Solms are Corporate Governance (Strategic and Operational), Policies, People, Best Practice, Legal, Certification, Insurance and Audit (Von Solms, 2001a). The list may not necessarily be complete, because there are no fixed boundaries to the dimensions.

A comprehensive Information Security management strategy should be based on a sound security architecture. This architecture "…is not something one can purchase. It is the process of developing an awareness of risk, an assessment of the current controls, and the alignment of controls to meet the requirements of the organisation…" (Tudor, 2001, p.23)

Tudor describes an Information Security Architecture as an 'architecture that should incorporate guidelines on Information Security Management, security policies and procedures, socio-ethical / cultural issues, risk management, user awareness and training, compliance and should be based on the sound implementation of security technology' (Tudor, 2001 p.1)

The first part of the paper will provide the reader with background information and propose a new architecture that can be used to manage and assess Information Security in a structured and holistic way.

The key role of digital forensics is the 'preservation, identification, extraction, documentation and interpretation of computer media for evidentiary and /or root cause analysis' (Kruse, 2004, p.1). In all abuse cases, protection of the evidence is both critical and central to the organization's ability to investigate and take action against the abuser (Sheldon, 2004).

The second part of the paper will define digital forensics, briefly discuss the relationship between Digital Forensics and Information Security and investigate if a DFMM should be part of an ISA.

2 BACKGROUND

Information Security must be managed on a macro-level, preferably by using an architecture that is based on an international best-practice and on micro-level using physical measurements in an organization with an established security culture.

Von Solms described Information Security as a multi-dimensional discipline, which involves in addition to technical security, other dimensions (Von Solms, 2001a). This paper will consider the following dimensions for Information Security: Corporate Governance – strategic and operational, Policies, People, Technology, Compliance, Risk Management and Legal dimension.

It is important to note that due to the dynamic nature of Information Security, the dimensions may overlap in terms of content. The graphical representation of the dimensions in figure 1 indicates the role of each dimension in the total security solution of an organization. All dimensions must exist and be integrated to have an effective security solution.

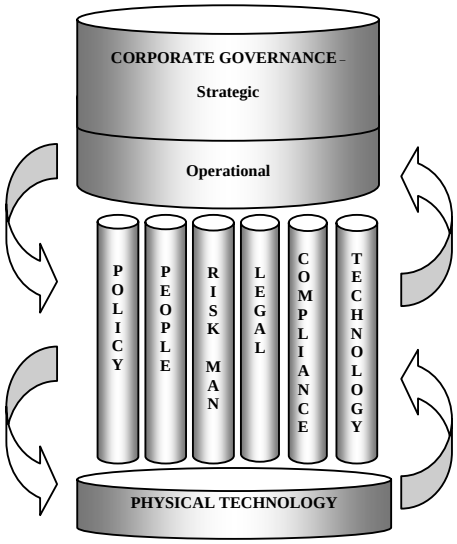

Figure 1 Dimensions of Information Security

Corporate Governance relates to the responsibilities of the Board of Directors and top management of a company (Von Solms, 2001b). According to the King II report, they are responsible for securing and protecting the information assets in a company (King, 2000). Corporate Governance is divided into strategic and operational governance.

All internationally accepted best practices for Information Security Management accept the formulation of policies as the starting point to implement Information Security in an organization. An Information Security policy will provide a framework for selecting and implementing countermeasures against threats (Eloff JHP, 2002a). The Policy dimension will cover all policies and propose that the organization should set up a policy framework.

The People dimension of Information Security is often neglected, but is crucial for the successful implementation of Information Security. This dimension includes user training and awareness programs. It is essential to create and maintain an Information Security culture in the organization. An effective and successful awareness and training program will create and maintain a 'human' firewall in an organization.

To manage the risks in an organization is critical for survival. Risk Management is more than risk assessment, it includes the consultation and communication with the outside world to get the latest information on types of risks, risk assessment, how to treat risks and the implementation of the countermeasures to control the risks.

The Legal dimension will incorporate the legal requirements as set out by government, statutory bodies and other relevant business partners.

Compliance is an essential dimension. This purpose of this dimension is to determine the success of the implementation of the Information Security strategy in the organization. It includes the audit procedures of the organization.

All the above-mentioned dimensions must be implemented on a sound foundation of relevant technology. Technology will be physical technology i.e. technical equipment like firewalls, logical technology for example access control software, operating systems, database management systems and the implementation of networks.

Various architectures for Information Security exist. The architectures studied and compared have the following common characteristics or elements:

- The architectures concentrate on general security implementation. Most architectures are based on a best practice e.g. ISO17799, use a multi-dimensional view by proposing security functions or controls that should be implemented on different management levels e.g. Strategic, Tactical and Operational levels. An integrated management strategy must support the architecture.
- Some of the architectures propose a multi-layered (onion) approach in the protection and use of the information resources (information, systems, networks and WWW connectivity) and emphasize the need to manage the 'Human' element in an organization with regards to Information Security. Organizations should create a human firewall by establishing a security culture.
- The architectures studied, do not consider the different dimensions of Information Security and do not provide a structured holistic blueprint to manage and assess the security posture of an organization. This paper will use elements of the existing architectures and the dimensions of Information Security to propose a new information security architecture - NISA.

3 A NEW INFORMATION SECURITY ARCHITECTURE

The aim of the new architecture is to have an integrated, holistic and structured approach to implement, manage and assess the various dimensions of Information Security while preserving the Confidentiality, Integrity and Availability of all information assets or resources of an organization by considering security functions within each dimension that needs to be implemented using technology or processes.

Existing architectures (Whitman, 2003) (Eloff JHP, 2002b) have identified different security functions on different management levels in an organization. The levels that will be used by the NISA are the management level, tactical level, and technical level.

Organizations implement security functions or controls to secure the information and information assets in the organization. Various security functions were identified from the literature studied. Additional functions, as prescribed by the ISO17799 and CobiT best practices are included in table 1, to obtain a comprehensive list of security functions.

The functions or controls can be associated to the different management levels. Table 1 allocates the functions to the management levels.

Table 1 Security functions associated with the management levels

Management	**Tactical**	**Technical**
Corporate Governance Security Culture Strategic Risk Management Security Management Strategic Information Security Plan Configuration Management	User Awareness Program • Awareness • Training Incident Response Plan Risk Assessment Business Continuity Plan Contingency Plan Disaster Recovery	Information Security services and mechanisms: • Identification and authentication • Authorization • Access control Technology: • Physical • Logical • Networks

Determine Requirements Organizational Structure Outsourcing Information Architecture Compliance Information Security Policy	Best Practices Personnel Security Standards, Procedures, Guidelines	• WWW connectivity Implementation Procedures

The list of functions in table 1 may not be complete. In some cases, the reader may disagree with the relevant placement of the functions, but this will not dramatically influence the work in this paper as it is important to demonstrate the concept of allocating a function to a management level. As Information Security is a multi-dimensional discipline, the various functions identified in the table 1 can be mapped to the different security dimensions in table 2.

Table 2 Security Functions mapped to Security Dimensions

Dimension	**Function**
Corporate Governance	Information Security Management Strategic Plan Organizational Plan Outsourcing Information Architecture Physical Security
Policies	Security Policy Standards, Procedures, Guidelines Best Practices
People	Security Culture Training and Awareness Program • Awareness • Training Incident Response Personnel Security

Risk Management	Risk Management Risk Assessment Business Continuity Plan Incident Response Plan Disaster Recovery Plan Access Control
Legal	Legal Compliance
Compliance	Security Audit Best Practices
Technology	Configuration Management Determine IT Requirements Information Security Services and Mechanisms • Access Control • Identification and Authentication Technology • Physical • Logical • Networks include www

The security functions within each dimension can be associated with the different management levels. Table 2 does not include a management level for every function. The level of the function can be obtained from the list of functions in table 1.

Figure 2 is a graphical representation of the security dimensions with associated functions within the management levels. Due to the number of functions involved, the functions per dimension are omitted from figure 2. The policy dimension has been extracted from figure 2 with the functions to demonstrate the concept of functions per management level.

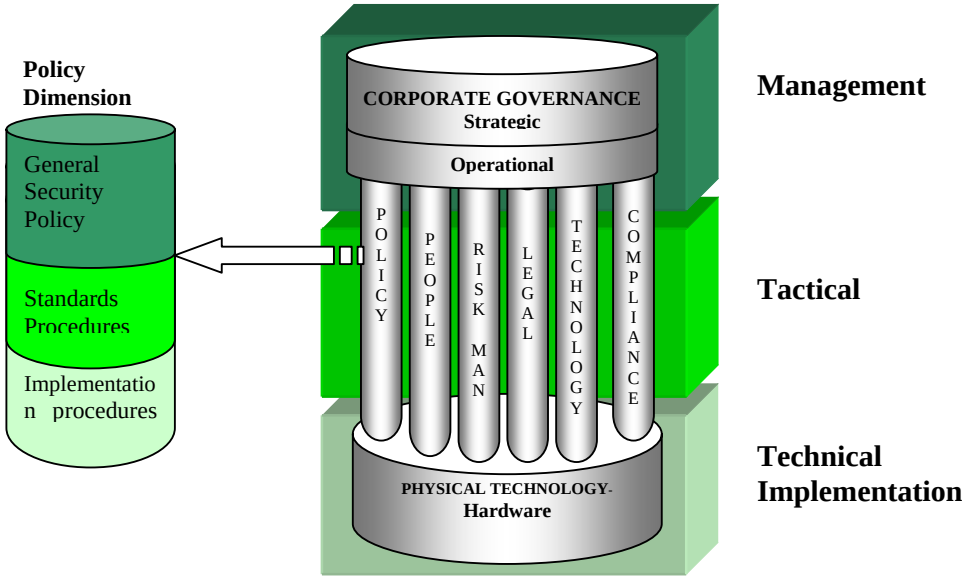

Figure 2 Dimensions mapped to the security management levels

The architecture includes technology as a vertical and a horizontal dimension as the dimension must be managed from a strategic management level to a technical implementation level. The basis for the implementation of security is the use of hardware – physical equipment (e.g. firewall).

The security functions presented in table 1 and table 2 must be implemented. The architecture distinguishes between processes and technology to implement security. Security processes will refer to all the Information Security Management functions that should be performed; for example setting up of an IT strategic security plan or the implementation of awareness programs. IT security technology will refer to all visible aspects of IT security. It will deal for example with access control and virus detection. Technology can be divided into 3 distinct areas (Eloff MM, 2000): physical technology (hardware), logical technology (software) and network technology (physical and logical).

The security implemented within the various dimensions will be using processes and / or technology. Figure 3 is a graphical representation of the implementation methods for security.

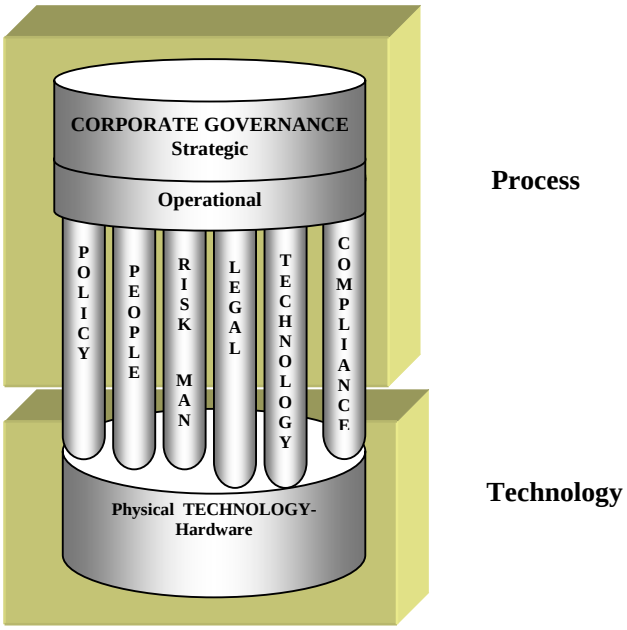

Figure 3 Implementation methods for security

The Corporate Governance, Policy, People, Risk Management, Compliance and Legal dimensions will implement controls by utilizing processes, whereas the technology dimension will require the implementation of technology and process controls.

The architecture recommends the securing of the following resources: Information, Systems – hardware and software, Networks including the Internet and People. Figure 4 is a graphical representation of the resources.

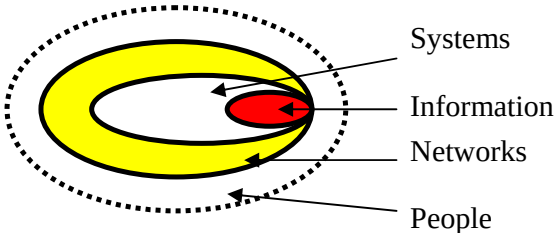

Figure 4 Graphical representation of resources

Information is the most important asset that needs to be protected from internal and external threats. Information can be directly accessed and used by people and systems and indirectly accessed and used by users or applications using networks and the Internet. All the resources exist in each dimension. When managing or assessing a dimension it is essential to consider all the resources.

4 COMPREHENSIVE VIEW OF NISA

The NISA will provide a holistic, integrated framework to implement, manage and assess Information Security in an organization. Figure 5 is a diagrammatic integrated view of the NISA.

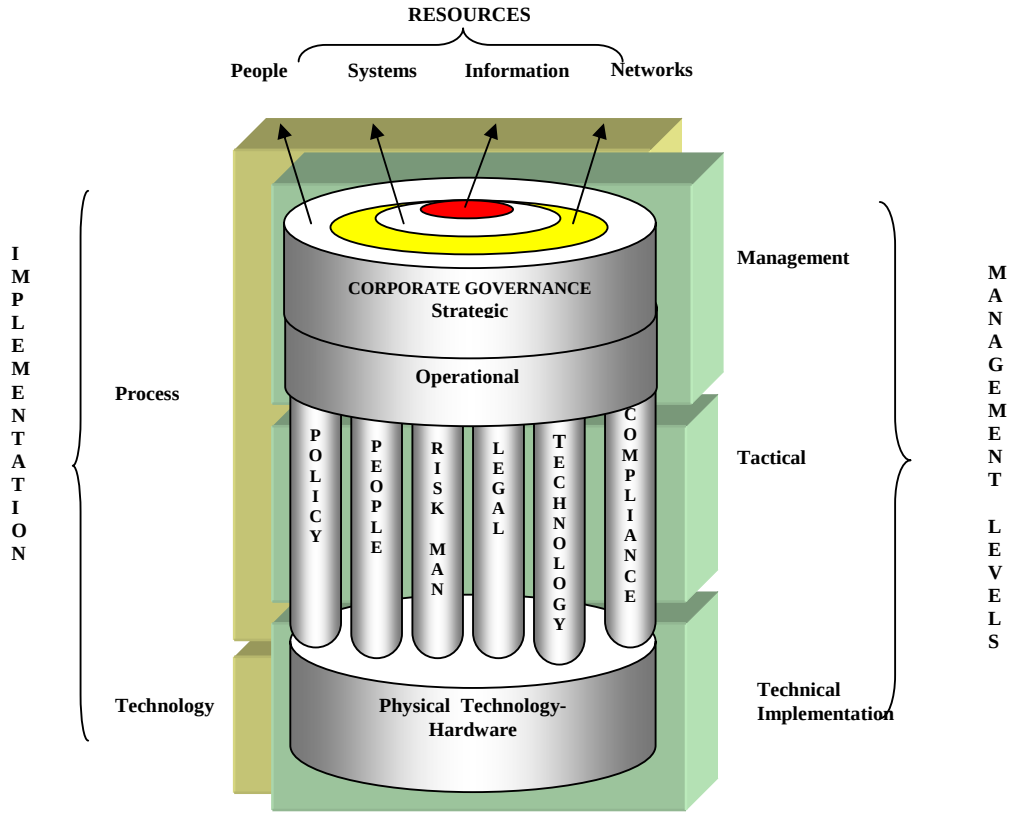

Figure 5 Diagrammatic integrated view of NISA

The architecture proposes three levels to implement, manage and assess security in the organization: management, tactical and technical implementation level. Each dimension of Information Security has different security functions, identified by existing architectures, ISO17799

and the CobiT best practice (Control Objectives for Information and related Technologies) on the different management levels, associated with it. Management can utilize processes and / or technology to implement, manage and assess the functions. It is important to consider all the resources when implementing a security function.

The advantages of the architecture are that

- it has simplified the implementation and management of security in an organization as it provides a clear direction on the most important dimensions of information security,
- it provides a list of functions that should be implemented on the various levels of management,
- it distinguish between processes and technology as implementation methods,
- all resources are considered, information, systems, networks and people,
- it is a flexible architecture that can be adjusted to suit the needs of the organization,
- it is a high-level integrated architecture based on best practices and
- an assessor can use the architecture to set up a high-level integrated assessment plan for the entire organization or a detailed assessment plan for a specific dimension. The assessor will assess the functions associated with each dimension to determine the security status of the dimension.

The disadvantages of the architecture are that

- the architecture has not been implemented and tested yet,
- the architecture does not supply implementation details,
- the functions listed may not be a complete list and
- the various dimensions may not be sufficient and organizations may spilt or add dimensions to address individual needs

It is important to note that all dimensions are interrelated and implementation and assessment plans for individual dimensions must provide for input from and output to the other related dimensions.

5 DIGITAL FORENSICS

The application of information technology as a tool enhances traditional methodologies. Organizations who apply computer systems as a business enabler, has improved the productivity and efficiency. Similarly has the introduction of computers as a criminal tool enhanced the criminal's ability to perform, hide, or otherwise aid unlawful or unethical activity. In particular, the surge of technical adeptness by the general population, coupled with anonymity, seems to encourage crimes using computer systems since there is a small chance of being prosecuted, let alone being caught (Reith, 2002). These "cyber-crimes" are not always new crimes, but rather traditional crimes translated into a cyber world by exploiting computing power and accessibility of information.

Digital forensics can be defined as "the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence derived from digital sources for the purpose of facilitation or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations" (Digital Forensic Research workshop, 2001) (Reith, 2002).

Digital forensics is important in today's modern day life as variety of digital devices exists that can be exploited in a criminal activity. Law enforcement is in an ongoing race with criminals in the application of digital technologies.

From the literature studied, there is a clear indication that many sophisticated forensic tools exits to assist with the acquiring of information, authentication of recovered evidence and the analysis of the data, various methodologies exist to conduct the investigation, but no comprehensive digital forensic management model exist. There is therefore a need in industry for a DFMM that will be scientifically sound and legally accepted. This model must ensure that the chain of evidence is maintained and that all evidence will be admissible in court.

Reith has proposed the following abstract forensics model / methodology (Reith, 2002):

1. Identification: Recognizing the incident from indicators and determine the type.
2. Preparation: Preparing tools, techniques, search warrants and monitoring authorizations and management support.
3. Approach strategy: Determine a suitable approach to maximize the collection of untainted evidence while minimizing the impact on the victim
4. Preservation: Isolate, secure and preserve the state of the evidence.
5. Collection: Record the physical scene and duplicate digital evidence using standardised and accepted procedures.
6. Examination: Systematic in-depth search of evidence relating to the suspected crime. Locate and identify possible evidence to construct detailed documentation.
7. Analysis: Determine the significance; reconstruct fragments of data to draw certain conclusions on evidence found.
8. Presentation: Summarize and explain the conclusions by using abstract terminology in a layperson's terms.
9. Returning evidence: Ensure that all physical and digital technology to the proper owner.

The methodology is on an abstract level, and can accommodate a wide variety of digital devices. The purpose of the model is to provide a consistent and standardised framework for digital forensic management. The chain of evidence of custody is inherent to the model.

It is also essential that when an incident has occurred, to determine the root-cause of the incident. This will ensure an even more secure environment. Further more is it necessary to determine who the perpetrator was and corrective steps should be taken against the individual. These corrective measures can include internal handling of the situation or the handing over of the incident to law enforcement, but you will need evidence that will be admissible in court.

Information security architectures on the other hand, focus on the prevention of security. When a security incident occurs, there are various systems in place to deal with the incident for example: intrusion detection systems, incident response plans as well as business continuity plans. However, incident response plans normally does not include forensic investigation guidelines and principles.

A forensic investigation should start as soon as an incident has been detected. Many organizations do not regard forensic investigations as a priority. The result is that the IT manager normally investigates the incident internally. This statement is supported by the CSI/ FBI 2004 survey that 70% of the respondents are patching up the holes of the breach and only 20% of respondent have reported the incidents to law enforcement agencies (Gordon, 2004).

The question arises whether Digital Forensics should be included in the NISA as a separate dimension or should it remain as a separate activity in the organization.

According to Wolfe, forensic security measures must be part of the organizations larger information security strategy (Wolfe, 2003). It should be incorporated into the NISA. If forensics is a separate dimension, one can determine the relationship of the dimension with the other dimensions. All dimensions will have references to and from the forensic dimension. One will have to include management strategies, policies, legal requirements, technology, compliance, people and risk management that are necessary for forensic investigations.

The forensic investigation will involve all the resources: People, networks, systems, information and also the physical environment. The investigator will use processes, procedures and technology to conduct the investigation.

In the past information security looked at the prevention and handling of incidents in an organization and forensics dealt with the post-mortem of the incidents. There is a need to develop new digital information security architecture deal with the challenges of digital forensics and cyber crimes.

6 SUMMARY

Information Security is a multi-dimensional discipline. The paper has identified the following dimensions of Information Security: Corporate Governance, Policy, Compliance, Legal, Risk Management, People and Technology.

Information Security Management should enable you to manage all the dimensions of Information Security while preserving the Confidentiality, Integrity and Availability of information and information assets. A well-defined architecture will provide a blueprint to manage the implementation of security in your organization effectively and efficiently.

The NISA is a comprehensive high-level architecture to guide management with the implementation and management of Information Security in an organization. The architecture will also provide management with a blueprint to manage and assess the security posture of the organization.

'Security begins with policy and ends with continuity plans that will facilitate recovery when all else fails' (Wolfe, 2003). Digital forensics should be an essential part of the strategic information security of an organization and further research is necessary to establish an integrated DFMM and ISA.

7 REFERENCES

BUSINESS IT AFRICA. (March 2001). *Security needs go beyond firewall*.

CULLERY A, (2003), *Computer forensics: past present and future, Information Security Technical report*, vol 8 nr 2, p32-35, Elsevier

GORDON LA, LOB M, etc. (2004). *CSI/FBI Computer Crime and security survey*,

DIGITAL FORENSIC RESEACH WORKSHOP, (2001), *A roadmap for Digital Forensics Research.* www.dfrws.org.

ELOFF JHP. (2002a). *What does international standards say on information security policies?* IT Security workshop.

ELOFF JHP. (2002b). *Implementing an IT infrastructure to fulfil your organizational objectives*:

IT security workshop.

ELOFF MM. (2000). *A Multi-dimensional model for Information Security Management*: PHD dissertation. RAU.

HUMAN FIREWALL COUNCIL. (2003*). Human firewall manifesto – a call to action*. http://www.humanfirewall.org/rfmwm.htm, August 2003.

INFORMATION SYSTEMS AUDIT AND CONTROL FOUNDATION. (1996). *Control Objectives for Information and Related Technologies*.

INTERNATIONAL STANDARDS ORGANIZATION. (1999). Website: http://www.iso.ch. Nov 1999.

KING II REPORT ON CORPORATE GOVERNANCE. (2000). Website: http://iodsa.co.za/lod%20Draft%20King%20Report.pdf, August 2003.

KRUSE II WARREN G.,JAY G HEISER. (2004). *Computer forensics incident response essentials*. Addison Wesley, Pearson Education.

REITH M, VARR V GUNCH G. (2002).*An examination of Digital Forensic Models*. International Journal of Digital Evidence Volume 1, Issue 3, http://www.ijde.org/docs/02 art2.pdf, (15/02/2005)

SABS ISO/IEC17799. (2001). SABS edition 11/ISO/IEC edition1, South African Standard, Code of practice for Information Security Management. South African Bureau of Standards.

SHELDON A, (2004), Forensic Auditing, *The role of computer forensics in the corporate toolbox*. http://www.itsecurity.com/papers/p11.htm (25/3/2004)

SINANGIN D, (2002), *Computer forensics investigations in a corporate environment*, Computer Fraud and Security Bulletin, 8, p.11-14, June 2002

TUDOR. Information Security architecture. (2001). Auerbach.

VON SOLMS SH. (2001a). *Information Security. A multi-dimensional discipline*, Computers and Security, volume 19, number 7. Elsevier.

VON SOLMS SH. (2001b). *Corporate Governance and Information Security*. Computers and Security Volume 20, number 3. Elsevier

WHITMAN M, MATFORD H. (2003). **Principles of Information Security**. Thompson Publishing.

WOLFE HB, (2003), *Computer Forensics*, Computer Security, 22, p 26-28