IT SECURITY PRACTICES IN AN ORGANIZATION: BALANCING TECHNOLOGY AND MANAGEMENT PERSPECTIVE

C Banerjee
Research Scholar, Jagannath University, Jaipur

Prof (Dr) PD Murarka
Professor, Arya Group of Colleges, Jaipur

Arpita Banerjee
Lecturer, St Xavier's College, Jaipur

Abstract

IT Security has long been considered a domain of technology. The hardcore IT specialists and technologists have been a source of influence in planning, designing, developing and implementing of IT security for organizations. IT security has been a matter of grave concern world wide since 1977 with reported incidents of security breaches like virus attacks, intrusion, spam emails, hacking, spoofing, phishing, SQL injection, DoS attacks, credit card and debit card misuse, identity theft, etc. As per recently available statistics, due to the unfortunate events of security breaches, globally, revenue losses have been reported which ranges from few million dollars to billions of dollars in some cases. Employing IT security has been traditionally seen as tantamount to technological afterthought overlooking the role of management practices. The above-mentioned evidences are adequate to establish the fact that management perspective should complement the technological aspect of IT security so that it can be applied in an organization in its entirety. The objective of this research paper is to explore and illustrate the evolving role and importance of employing management practices together with technological practices in IT security. The research paper highlights various established management practices and models associated with IT security along with their limitations through the help of recent published work. In addition, the areas that need further investigations are also identified in this paper.

Introduction

In today's information age, millions of people use software and applications to perform personal, business and professional activities bearing in mind that the software they use is reliable and trustworthy and operations they perform are secured. The world's economy depends on the coordinated and secured use of software which nowadays is considered to be an essential and integral part of everyday life. Security brings value to organizational units through use of software in terms of people's trust. Software is attacked intentionally to get hold of sensitive and highly important information. This results in breaches in security, organization's reputation and most importantly people's trust. The sole intention of the attacker is to carry out well funded, destructive and unethical objectives that could cause harm and damage to individuals, organizations, nations and the world at large (Banerjee 123-128).

Although, *risk* and *business* are two terms which are considered to be undividable, still, when it comes to security risk to data and information, unidentified challenges arise for organizations and government equally. Significant contributions are put forward by the technology community in terms of preventive, defensive and reactive methods and controls as a mitigation mechanism against security infringement. A number of security standards are also defined containing a set of security policies, procedures and guidelines which complement security methods and controls and aid security management. The technological approach and management approach as a separate individual unit to security of information has proven to be insufficient and there has been a rise in security incidents over the years (Johnson and Dimitriadis 16-24).

When it comes to implementing security in information and technology domain, the role of IT specialist has always been considered to be of utmost importance and a lack of management perspective to implementation of security is present. Although researchers have done remarkable work in the field of security and its responsibility in information and technology, still, much work needs to be carried out in order to make software more secure and reliable by a blend and synchronization of the technology perspective with management perspective. Extending the work carried out earlier, in this paper we intend to explore and illustrate the evolving role and importance of employing management practices together with technological practices in IT security. The rest of the paper is organized as follows: Section II highlights the importance of IT security from technology and management perspective, and section III, presents the review of literature as a brief overview of various established IT security standards, methods, and models along with its limitations. Section IV discusses the objective of our research work, and Section V focuses on the areas that need further investigations. 'Conclusion and Future Work' are given in Section VI.

Importance of It Security: Technology versus Management Perspective

Before proceeding further, we need to understand what security is? Security is a degree of protection where a separation is created between assets and threats (Schneier). The chief attributes which contribute to the security of information technology, includes Confidentiality, Integrity and Availability. Confidentiality is maintaining the privacy of the people and their information by preventing the disclosure of information to unauthorized system. Integrity ensures that data cannot be modified untraceably. Availability guarantees that the information must be made available whenever it is needed (Tipton and Krause). Now, we will discuss IT security from both technology as well as management perspective as follows:

It Security from Technology Perspective

In the IT realm, security exists as software security, computer security, data security, information security, web security and network security (Schneier). Software security also called application security includes procedures adopted throughout the software development process to minimize or prevent threats and attacks resulting due to exploits and vulnerabilities present owing to the flaws introduced or kept in the software during the requirements, design, development, deployment and maintenance phase of the software (McGraw). Data Security comprises of protection of database(s) from unwanted actions of unauthorized users (Glass 495-506).

Computer security encompasses information and assets protection from theft, corruption, or natural disaster, while allowing it to remain accessible and productive to its intended users (Bishop 67-69).

Information security includes protection of information and its system from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction (Tipton and Krause). Network

security encompasses various provisions and policies taken by network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources (Stallings).

Web security includes the objective to establish rules and measures to use against attacks over the Internet (Chakrabarti 13-21). Security controls such as firewalls, antivirus, data encryption mechanisms, digital signatures, digital certificates, data backup procedures, access control mechanisms, intrusion detection systems, secured software development models and methodologies, biometric systems, etc. are used for security of IT from technology perspective (Dimitriadis).

It Security from Management Perspective

Standards are principles which are established means of determining the quality of a practice or procedure when used as a model. Standard can also be defined as approved policies which can be monitored for compliance by an authority as a minimum acceptable benchmark. They guide decisions and help in achieving a rational outcome. Within an organization, the policy is adopted at a top management level and procedures are made to work at middle management level (Crook). It is a well-known fact that standards are important for the healthy growth of an organization (Role of Standards: A guide for small and medium-sized enterprises). For doing successful and productive operations in a business, we need standards. In a similar fashion, to implement security for information technology, an organization needs to adopt a model in the form of policies, guidelines, and procedures to standardize its secured operations.

To ensure proper security, the focus of an organization should be on the people and its management more than on technology. It is statistically proven that IT security administration is a management issue and not purely a technical issue. It is also stated that in IT security, 1/3rd of the time is spent on the tackling of technical issues and 2/3rd of the remaining time is spent on developing policies and procedures, performing security reviews and risk management, addressing contingency plans and on promotion of security awareness. Hence it is recommended that an organization needs to adopt a systematic approach for identification, assessment and management of information security threats and risk in the form of Information Security Management (ISM) (Rezakhani 4-8).

An organization needs a system for implementation of security standards often called Information Security Management System (ISMS). An ISMS is defined as a coherent set of policies for the implementation of information security management (Vacca). Since standards provides a theoretical way to solve a practical problem, hence, to practice such theories, i.e., to bridge the gap between theory and practical, the management of information security should be equipped with a sound maturity model like CMMI (Capability Maturity Model Integration), ISO (International Standardization Organization), ITIL (IT Infrastructure Library), etc. (Aceituno).

To address the issue of information security of an organization, a number of governments and institutes have developed a number of models and standards based on ISMS framework, which are readily available in the market for its adoption into the system. Organizations and Institutions like NIST, ISO/IEC, ITIL, etc. have developed and provided a number of Information Security standards and guidelines and have also proposed security models for their implementation in an organization. Although a number of information security standards exists, but an organization can derive profit only if these standards are implemented in a proper way (Thompson).

Combining Technology and Management Aspect of It

The technology perspective of IT security is more a concern with the tactical aspect which equates to technical requirements only. The management perspective of IT security focuses on the strategic aspect which equate to management requirements only (Seeholzer, pp.144-161). Every organization has specific business needs and to embed the information security into an organization, a detailed analysis of that organization becomes a necessity (Dimitriadis). Moreover, senior management, practitioners of information security and technology people should be made aware that a team effort and cooperation at all levels is required to secure the assets of an organization (Banerjee, pp.1-5).

Literature Review: Information Security Standard, Models and Methods

Many standards, models and methods have been proposed by many research organizations and institutions for security implementation taking into consideration the management perspective together with technical perspective but the latter seems to overpower the former in almost every case. The current standards of information security and management can be classified as process oriented like CMMI, ISO 9001:2000, ITIL/ITSM, control oriented like ISO13335-4, product oriented like common criteria, risk analysis oriented like OCTAVE, and best practice oriented like COBIT, ISO/IEC 17799:2000 (Aceituno). We present here a brief review of the various standards, models and methods currently being used for implementation of IT security in an organization:

Standards for Information Security Management

Looking into the present-day and future scenario, awareness has to be created among organizations for a need to dedicate more resources for the protection of information assets. For addressing the issues of information security and management, standards are laid down by organizations and institutions. Some of the commonly applicable standards in information security and management are summarized below:

ISO Standards

International Organization for Standardization (ISO) established in 1947 collaborated with International Electrotechnical Commission (IEC) and International Telecommunication Union (ITU) on Information and Communication Technology (ICT) standards. Some of the significant standards laid down by ISO/ IEC are as follows:

Some of the published standards

ISO/IEC Standards	Area(s) addressed
ISO/IEC 27000	Includes overview and vocabulary of Information security management systems (ISMS)
ISO/IEC 27001	Covers requirements related to ISMS
ISO/IEC 27002	Code of practice for information security management
ISO/IEC 27003	Provides implementation guidelines for ISMS
ISO/IEC 27004	Contains measurement of Information security management

ISO/IEC 27005	Covers Information security risk management
ISO/IEC 27006	Includes requirements for bodies providing ISMS audit / certification
ISO/IEC 27010	Provides Security techniques for IT and Information security management for inter-sector and inter-organizational communications
ISO/IEC 27011	Provides Information security management guidelines for telecommunications organizations based on ISO/IEC 27002
ISO/IEC 27031	Provides Guidelines for information and communications technology readiness for business continuity
ISO/IEC 27033-1	Includes overview and concepts of Network security
ISO/IEC 27035	Covers Security incident management

Source: http://en.wikipedia.org/wiki/ISO/IEC_27000-series

Some of the standards under publication

ISO/IEC Standards	Area(s) addressed
ISO/IEC 27007	Provides ISMS auditing guidelines with focus on management system
ISO/IEC 27008	Includes guidance for auditors on ISMS controls with focus on the information security controls
ISO/IEC 27013	Contains guideline on the integrated implementation of ISO/IEC 20000-1 and ISO/IEC 27001
ISO/IEC 27014	Provides a framework for Information security governance
ISO/IEC 27015	Provides Information security management guidelines for the finance and insurance sectors
ISO/IEC 27032	Includes guideline for Cyber Security
ISO/IEC 27033	Covers IT network security, a multi-part standard based on ISO/IEC 18028:2006
ISO/IEC 27034	Provides guideline for application security
ISO/IEC 27036	Includes guidelines for security of outsourcing
ISO/IEC 27037	Offers guidelines for identification, collection and/or acquisition and preservation of digital evidence

Source: http://en.wikipedia.org/wiki/ISO/IEC_27000-series

Apart from the ISO/IEC security standards mentioned above in tabular format, ISO/IEC 15408, is also called Common Criteria. It is a standard for evaluation criteria for IT security and constitutes three components, viz., ISO/IEC 15408-1:2005 which includes introduction and general models, ISO/IEC 15408-1:2005 which comprises of security functional requirements, and ISO/IEC 15408:3:2005 which contains requirements for security assurance. Further, ISO/IEC 13335 standard focuses on the IT security management and comprises

of four components, viz., ISO/IEC 13335-1:2004 which contains concepts and models for information and communication technology security management, ISO/IEC 13335:3:1998 which comprises of techniques for management of IT security, ISO/IEC 13335-4:2000 which focuses on technical security controls, and ISO/IEC 13335-5:2001 which covers network security management guidance (Djouab 3231-3239)

National Institute of Science and Technology (NIST)

National Institute of Science and Technology (NIST) founded in 1901 is a non-regulatory federal agency within the U.S. Department of Commerce. NIST promotes innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

Some of the standards which are published by NIST are given below with areas they intend to addressed related to IT security management:

NIST Standards	Area(s) addressed
SP 800-137	IS Continuous Monitoring for Federal IS and Organizations
SP 800-115	Technical Guide to Information Security Testing and Assessment
SP 800-100	Information Security Handbook: A Guide for Managers
SP 800-60 Rev. 1	Guide for Mapping Types of Information and IS to Security Categories: (2 Volumes)
SP 800-59	Guideline for Identifying an IS as a National Security System
SP 800-53 Rev. 4	DRAFT Security and Privacy Controls for Federal Information Systems and Organizations
SP 800-50	Building an IT Security Awareness and Training Program
SP 800-47	Security Guide for Interconnecting Information Technology Systems
SP 800-39	Managing Information Security Risk: Organization, Mission, and Information System View
SP 800-37 Rev. 1	Guide for applying Risk Management Framework to Federal IS
SP 800-36	Guide to Selecting Information Technology Security Products
SP 800-35	Guide to Information Technology Security Services
SP 800-32	Underlying Technical Models for Information Technology Security
SP 800-30 Rev. 1	Guide for Conducting Risk Assessments
SP 800-27 Rev. A	Engineering Principles for Information Technology Security
SP 800-14	Generally Accepted Principles and Practices for Securing IT Systems

Source: http://csrc.nist.gov/publications/PubsSPs.html

ISACA

ISACA previously known as Information Systems Audit and Control Association was founded in 1967 in the USA. It is an international professional association that deals with IT governance. ISACA has co-developed standards, guidelines and procedures for the auditing of information system along with the International Federation of Accountants (ISACA). ISACA has created a framework named Control Objectives for Information and Related Technology (COBIT) 5 in 2012 for information technology (IT) management and IT governance which allows managers to bridge the gap between control requirements, technical issues and business risks (Abu-Musa 99-126; Susanto 23-29).

Information Technology Infrastructure Library (ITIL)

Information Technology Infrastructure Library (ITIL) published between 1989 and 1995 in the UK on behalf of the Central Communications and Telecommunications Agency (CCTA) is a set of practices for IT service management with focal point on aligning IT services with the business needs as shown in the figure 1.1. given below. Presently ITIL v3 is in use by many organizations worldwide (Susanto 23-29; Cartlidge)

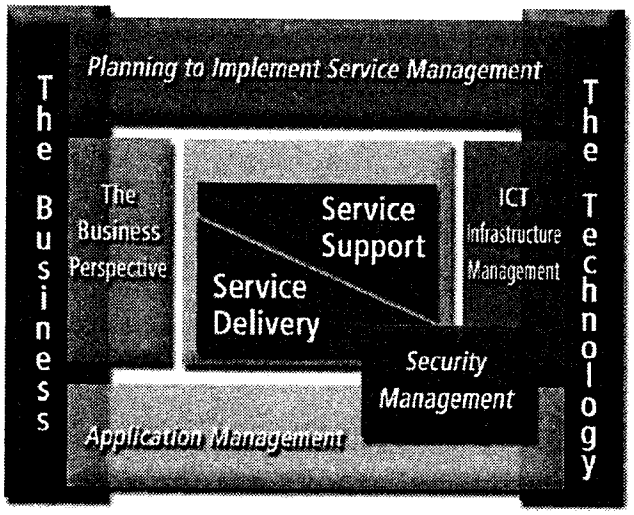

Figure 1.1: ITIL showing alignment of Management and Technology Aspects

Source: http://www.ijens.org/vol_11_i_05/113505-6969-ijecs-ijens.pdf

Maturity Models for Information Security Management

Information security maturity model is intended to be used as a tool for evaluation of organization's ability to meet the objectives of security. If properly used it ensures the mapping of security requirements with the business goals. A sound information security maturity model addresses four domains, viz., organization governance, organizational culture, the architecture of the systems, and service management which affects the security in an organization and helps an organization to identify and explore strength and weakness of its security aspect (Saleh 316-337).

Below we present a brief outline of various information security management maturity models.

Capability Maturity Model Integration (CMMI)

Capability Maturity Model Integration (CMMI), a successor of CMM, is developed by Software Engineering Institute (SEI), Carnegie Mellon. It is a suite of products used for process improvement as shown below in figure 1.2.

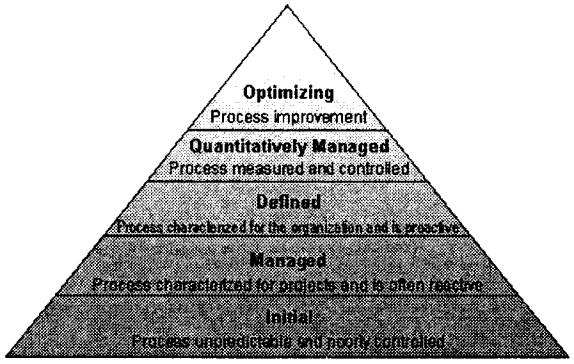

Figure 1.2: Five Stages (Levels) of CMMI Model

It has two representation layers, viz., continuous and staged representation. Continuous representation has 6 capability levels and allows organization to select a process area and improve processes related to it. Staged representation includes 5 maturity levels and uses predefined sets of process areas to define an improvement path for an organization. The organizational benefits of CMMI are shown in the figure 1.3 given below (Chen; West; Shrum; Spence; Constantinescu).

Performance Category	Median Improvement
Cost	34%
Schedule	50%
Productivity	61%
Quality	48%
Customer Satisfaction	14%
Return on Investment	4:1

Figure 1.3: Organization Performance of CMMI

The technical benefits of CMMI are that it provides more detailed coverage of the product life cycle, provides a set of well-integrated models that facilitate project management and improves the development process, promotes collaboration between system engineering and software engineering and it has the better ability to address scalability.

ISM3

The foundation of ISM3 has been laid taking into account the best ideas of management systems and controls from ISO 9000, ITIL, CMMI and ISO 27001. It can be used both at an entry level by small organizations and at a sophisticated level by major organizations as part of their governance assurance processes. It comprises of four conceptual models, viz., information security management model, organization model, information system model and security-in-context model. The business focus of ISM3 is shown in figure 1.4.

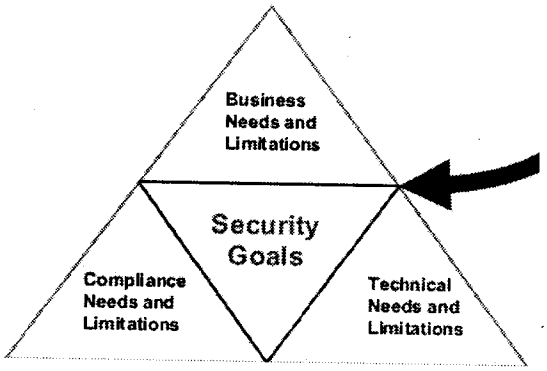

Figure 1.4 Showing Business Focus of ISM3

Every ISM3 process has a rationale section, which expresses how the process contributes to the goals of the operational, tactical, and strategic level. ISM3 is a complete standard that is business-friendly, adaptable, creditable, compatible, scalable and open (Narayanan).

Methods for Information Security Management

There are a number of methods available for information security management like OWASP CLASP (Comprehensive, Lightweight Application Security Process), Microsoft SDL (Secure Development Lifecycle), Macgraw's Touchpoint, etc. but they only provide a well-organized and structured approach for moving security concerns into the early stages of software development process. These methods use a prescriptive approach and help organizations to document activities. They are more technology oriented and much focus and work in needed to explore their management aspect (De Win).

Limitations

The majority of the information security standards are suitable for large organizations and medium-sized as well as small organizations often have difficulty in adopting them. Due to this the objective of security and its alignment to business needs cannot be achieved in totality with respect to organization size. Also a pessimistic view by smaller organizations in terms of cost, documentation and bureaucracy is taken for implementation of standards. They also find it difficult to relate standards to their business needs and to justify the application of the international standards in their operations. There are many misconceptions about the implementation of standards like standards force people to change their methods, standards reduce productivity by forcing unnecessary actions, major time and effort is required for its implementation. A major shift in organizational culture and attitude of people involved is required (West; Shrum; Spence; Constantinescu; Higgins).

From the literature review, it is evident that most of the information security management maturity models utilize the process-centric method of assessment and not much work in done in other aspects like product centric method of assessment, control centric and risk assessment centric. This information security management maturity model also does not address the threat issues like human error, incompetence, fraud and corruption (Narayanan).

As per the facts stated above, the information security models are more technology oriented and the researchers need to work on combining the strong points of all approaches in order to distill an improved, consolidated and secure development life-cycle process. Complementary activities may be selected in order to improve the overall coverage of the process. Finally, the management aspect needs to explore to fit it in any kind of organization (De Win 1152-1171).

Objectives of Research Work

The objective to the research work which is being carried out is to provide an initial platform through which any organization can achieves the following:

- Ensure that an adequate level of security is attained.
- Make optimum use of technology and management security resources.
- Help an organization adopt best security practice irrespective of its specific needs.
- Help bridge the gap between technology and management people by making the technology people understand that they cannot possibly cover all areas of IT security and the management people understand the importance and value of information security.
- Aid in the development of an organizational subculture of information security for managing the people factor concerned with information security.
- Make it clear that strategy (management perspective) and tactics (technology perspective) work in synchronized coordination and are complementary to each other.
- Promote the use of Information Security Management System in an organization.
- Support the use of Maturity Model in Information Security Management System for bridging the gap between the theoretical and practical aspects of security standards.

Areas That Need Further Investigations

Some of the key areas that need further investigation by the research community include the following:

- The information security standards, maturity models and methods need to be improved and revised to include active role and acceptance of medium and small organizations.
- A coordinated and synchronized approach need to develop between the various standards, maturity models and methods dedicated to information security keeping in mind all sizes of organization.
- The time and efforts invested for the implementation of information security and its management needs to be reduced.

- The impacts of the shifting organization culture due to its implementation needs to be addressed with one-to-one mapping of the process areas as per organizational requirements.
- Some metrics should be developed to measure the behavioral aspect of an organization.
- Active participation of aspects like product-centric method of assessment; control-centric and risk-assessment-centric features while designing and developing ISMM models is needed.
- The ISMM model can be improvised for addressing threat issues like human error, incompetence, fraud and corruption by means of organizational security culture.
- The management aspects of various information security methods needs to be explored and addressed in future.

Conclusion and Future Work

It is evident from the research findings that although a number of information security standards, maturity models and methods are available, still there are reported incidents of security breaches targeted by outsiders as well as insiders worldwide. The paper tried to present the importance of information security from technology and management perspective. It also showed critical review of various information security standards, maturity model and methods and their related role in implementation of security in an organization with their limitations. At the same time, a number of noteworthy research areas are also identified for further investigations in the concerned area. The paper will help the researchers who want to pursue their research in information security management by providing a brief but complete review on the existing literature along with the current research topics. The paper will serve as a base paper for other researchers who will choose the research topics through our paper.

Future work may include design and development of a concrete security standard which will aid in a more coordinated, synchronized and secure maturity model. This model in turn will help in aligning the security and business needs with the allied security methods for balancing the technology and management perspective of security of an organization. This work will surely help the industry to have a more holistic, coordinated, consistent and synchronized approach to technology and management aspect which drive the organizations to achieve optimum security in the field of Information Technology.

Works Cited

Abu-Musa, Ahmad A. "Exploring COBIT Processes for ITG in Saudi Organizations: An empirical Study." *The International Journal of Digital Accounting Research* 9 (2009): 99-126.

Aceituno Canal, Vicente. "ISM3 1.0 Information Security Management Maturity Model." Institute for Security and Open Methodologies, 2004. Web. 15th Jan 2013 <http://trygstad.rice.iit.edu:8000/Policies%20&%20Tools/ISM3_1.0_InformationSecurityManagementMaturityModel.pdf>

---. Vicente. "Usefulness of an Information Security Management Maturity Model." *Information Systems Control Journal* (ISACA) 2 (2008).

Altena, J. A. "ISO/IEC 27002 Baseline Selection Control selection based on effectiveness and cost within a fixed budget.", Education Institute Computing and Information Sciences. (Jul 2012).

Banerjee, C and S K Pandey. "Software Security Rules: SDLC Perspective." *International Journal of Computer Science and Information Security (IJCSIS)* 6.1 (Oct 2009): 123-128.

---. "Research on Software Security Awareness: Problems and Prospects." ACM SIGSOFT SEN 35.5 (Sep 2010): 1-5.

Bishop, Matt. "What is computer security?" *Security & Privacy,* IEEE 1.1 (2003), 67-69.

Cartlidge , Alison et. al. "An Introductory Overview of ITIL® V3." The UK Chapter of the it SMF, 2007. Web. 15th Jan 2013 <http://www.best-management-practice.com/gempdf/itSMF_An_Introductory_Overview_of_ITIL_V3.pdf>.

Chakrabarti, Aniraban, and G. Manimaran. "Internet Infrastructure Security: A Taxonomy." *Network* – IEEE 16.6 (2002): 13-21.

Chen, Yen, Elizabeth Myers, and Stephanie Sornatale. "Capability Maturity Model Integration (CMMI)." author STREAM. Web. 14th Jan 2013 <http://www.authorstream.com /Presentation/aSGuest42351-366154-capability-maturity-model-final-software-engine ering-education-ppt-powerpoint/>

Constantinescu, Radu, and Ioan Mihnea Iacob. "Capability Maturity Model Integration." *Journal of Applied Quantitative Methods* 2.1 (2007): 187.

Crook, Robert, Ince Darrel, and Nuseibeh Bashar. "Towards an analytical role modelling framework for security requirements." Proc. of the 8th International Workshop on Requirements Engineering: Foundation for Software Quality (REFSQ'02), 2002.

De Win, Bart, et al. "On the secure software development process: CLASP, SDL and Touchpoints compared." *Information and Software Technology* 51.7 (2009): 1152-1171.

Dimitriadis, Christos. "Information Security from a Business Perspective.", *IT Business Edge Network.* Quinstreet Enterprise, 2011. Web. 14 Jan 2013 <http://www.itbusinessedge.com/cm/community/features/guestopinions/blog/information-security-from-a-business-perspective/?cs=45475>

Djouab, R. "An ISO/IEC standards-based quality requirement definition approach: Applicative analysis of three quality requirements definition methods." IEEE International Symposium on Industrial Electronics. (Jul 2006): 3231–3239.

Glass, Robert L., Vessey Iris, and Ramesh Venkataraman. "Research in software engineering: An analysis of the literature." *Information and Software Technology* 44.8 (2002): 491-506.

Higgins, Sarah. "Information Security Management: THE ISO 27000 (ISO 27K) SERIES." Digital Curation Centre (DCC), 19 March 2009 Web. 15th Jan 2013 <http://www.dcc.ac.uk/resources/briefing-papers/standards-watch-papers/information-security-management-iso-27000-iso-27k-s>

ISACA. Standards, "Guidelines and Procedures for information system auditing." ISACA, 2013. Web. 15th Jan 2013 <http://www.isaca.org/Knowledge-Center/Standards/Documents/ALL-IT-Standards-Guidelines-and-Tools.pdf>

Johnson, Eric M. and Goetz Eric. "Embedding Information Security into the Organization." *IEEE Security and Privacy* 5.3 (May 2007): 16-24.

Malik, F Saleh. "Information Security Maturity Model." *International Journal of Computer Science and Security (IJCSS)* 5.3 (2011): 316-337.

McGraw, Gary. "Software Security." *IEEE Security & Privacy.* Vol. 2, no. 2, pp. 80-83, March-April 2004, doi:10.1109/MSECP.2004.1281254.

Narayanan, Anup. "Think Beyond "Controls": A "Process"-based Approach for Information Security Management using ISM3." Web. 15th Jan 2013 <http://www.anupnarayanan.org/ismsusingism3.pdf>

Rezakhani, Afshin, AbdolMajid Hajebi, and Nasibe Mohammadi. "Standardization of all Information Security Management Systems. *International Journal of Computer Applications* 18.8 (Mar 2011): 4-8.

Schneier, Bruse. "Beyond Fear." *Thinking Sensibly about Security in an Uncertain World.* Springer-Verlag New York Inc.: Copernicus Books. 2003.

Seeholzer, Roger. "Information Security Strategy: In Search of a Role." *18th Americas Conference on Information Systems," AMCIS* (Aug 2012): 144-161. Web. 14th Jan 2013 <http://aisel.aisnet.org/amcis2012/proceedings/ISSecurity/24>

Shrum, Sandy, and Mike Phillips. *CMMI Overview for Executives.* Pittsburg: Software

Soto, Corpuz Maria. "Limitations of the Information Security Management System Assessment Approaches in the Context of Information Security Policy Assessment." Information Security Institute, Web. 15th Jan 2013 <http://www.iiis.org/CDs2010 /CD2010SCI/R M C I _ 2 0 1 0 / P a p e r s P d f / RA512UO.pdf>

Spence, Peter, Brenda Andrews, and Walter Miller. "Capability Maturity Model Integration (CMMI) Debrief." docstoc, 2004. Web. 15th Jan 2013 <http://www.docstoc.com/docs/46697447/Capability-Maturity-Model-Integration-CMMI-Debrief-July-15-2004-Peter-Spence-Brenda-Andrews-Walter-Miller-CMMI-Debrief-CMMI-provides-guidance-for-im>

Stallings, William. *Network Security Essentials – Applications and Standards.* 4th ed. USA: Pearson Education India, 2007.

---. "Standards for Information Security Management." *The Internet Protocol Journal.* CISCO Systems Inc. 10.4 (2007).

Susanto, Heru, Nabil Almunawar Mohammad, and Yong Chee Tuan. "Information Security Management System Standards: A Comparative Study of the Big Five." *International Journal of Electrical and Computer Sciences IJECS-IJENS* 11.5 (Oct 2011): 23-29.

Thompson, Kerry. "The Best Guides for Information Security Management." *SysAdmin Magazine* June 2007. Web. 14th Jan 2013 <http://www.crypt.gen.nz/papers/infosec_guides.html>

Tipton, Harold F., and Krause Micki. *Information Security Management Handbook.* 6th ed. USA: Auerbach Publications, CRC Press, 2007.

United Nations Industrial Development Organization. "Role of Standards: A Guide for Small and Medium-Sized Enterprises." UNIDO, 2006. Web. 14th Jan 2013 <http://www.unido.org/fileadmin/media/documents/pdf/tcb_role_standards.pdf>

Vacca, John R. *Computer and Information Security – Handbook.* USA: Morgan Kauffman Publishers, Elsevier, 2009.

West, Michael. *Real Process Improvement Using CMMI,* USA: Auernach Publications. 2004.