Enterprise Information Security Policy Assessment - An Extended Framework for Metrics Development Utilising the Goal-Question-Metric Approach

Maria Soto Corpuz
Information Security Institute, Queensland University of Technology
Brisbane, Queensland/4000, Australia

ABSTRACT

Effective enterprise information security policy management requires review and assessment activities to ensure information security policies are aligned with business goals and objectives. As security policy management involves the elements of policy development process and the security policy as output, the context for security policy assessment requires goal-based metrics for these two elements. However, the current security management assessment methods only provide checklist types of assessment that are predefined by industry best practices and do not allow for developing specific goal-based metrics. Utilizing theories drawn from literature, this paper proposes the Enterprise Information Security Policy Assessment approach that expands on the Goal-Question-Metric (GQM) approach. The proposed assessment approach is then applied in a case scenario example to illustrate a practical application. It is shown that the proposed framework addresses the requirement for developing assessment metrics and allows for the concurrent undertaking of process-based and product-based assessment. Recommendations for further research activities include the conduct of empirical research to validate the propositions and the practical application of the proposed assessment approach in case studies to provide opportunities to introduce further enhancements to the approach.

Keywords: information security policy; information security management assessment; security policy assessment; security assessment

1. INTRODUCTION

Organizations develop enterprise information security policy to provide strategic direction in implementing their information security management programs [1][2][3][4][5][6]. The enterprise information security policy (herein referred to as security policy in this paper) defines information security program goals, assigns responsibilities and sets security control requirements [1][7] based on corporate business and risk management objectives [3][4][5]. It is a major element of an organization's corporate governance [8] and risk management strategy [9].

The development and management of security policies are required for the effective governance and implementation of information security [6][10][11]. Effective information security policy management requires policy review activities in addition to policy development and implementation [6][7][8][9] to address evolving risk exposures [2] and provide risk assurance to organizations. However, as will be presented in this paper, limitations in information security assessment methods include the lack of a measurement methodology that facilitates metric development [12].

In addressing these limitations, Section 2 first discusses the required considerations for security policy development and the contextual elements of security policy assessment. Section 3 then presents a review of the current security management assessment methods in the context of security policy assessment. In Section 4, the Enterprise Information Security Policy, a security policy assessment framework that expands on the Goal-Question-Metric approach (GQM) [13] is proposed. This is followed by Section 5 which presents a case scenario example to illustrate a practical application of the proposed policy assessment approach. Lastly, conclusions and recommendations for further research are provided in Section 6.

2. ENTERPRISE INFORMATION SECURITY POLICY ASSESSMENT

An assessment is a data gathering exercise conducted as an element of a learning process the results of which are used to review and revise an organization's objectives and strategies [14]. Assessments are undertaken in regular pre-defined periods to establish the stages of improvement (or degradation) in learning.

Information security assessments commonly take on the perspective defined by the information security management standards [3][4][5][15] and are conducted mainly as a requirement to evaluate organizational compliance to legislation and mandatory standards. The drivers for information security policy management include the need for IT governance [9][16][17], the requirement for regulatory compliance [18] and risk management [2].

The major considerations for developing and managing security policies that are defined and cited by the security policy management frameworks [6][11][19] and the best practice guidelines [1][2][3][4][5][6]include the following:

1) Contextual business alignment [2][7][16][19][20] – it is a requirement for policy development process to be aligned with corporate business and/or organizational requirements such as corporate governance and risk management;
2) Integrated security policy structure [5][6][21] - the outcome of the development process should result in product set of security policies, practices and procedures

that are coordinated and integrated and implemented at different levels;

3) Cost-efficient implementation [22][23] – implementation and enforcement of security policies should be balanced between cost and benefits; and
4) Continuous improvement management [2][24] – development process should facilitate policies to be continually reassessed and updated to address evolving risks.

The drivers and the policy characteristics comprise the contextual elements for security policy assessment. These assessment elements are considered in defining the domains of security policy assessment and evaluating assessment methods which are presented and discussed in the next section.

Domains of Security Policy Assessment

The elements of an assessment activity usually consist of a defined purpose and method of measurement [25] and which involves metrics development [26]. The purpose or requirement for assessment defines the method of measurement and the metrics approach. Management of security policies requires both the establishment of a policy development process and the effective implementation of the product set of security policies. For this paper, a security policy assessment method may be classified as either a process-based approach or a product-based approach. The process-based approach is utilized if the primary assessment objective is business process improvement whereas the product-based assessment approach is utilized if effectiveness of security policy implementation is the primary assessment concern [12].

Process-based Assessment: A driver for utilizing process-based assessment is the requirement for business improvement drawn from the corporate need for improving business performance and productivity [27]. Such requirements for process assessment are usually brought about by organisational changes in corporate structure, strategic business direction and overall corporate objectives [28]. These changes impact the implementation of strategic aspects of corporate governance such as information security.Research literature has indicated that information security has become a major part of corporate governance [1][3][8] that focuses more on people, processes and information in addition to IT [9]. As the security policy provides the critical direction-setting aspect of information security, it is one of the most important controls of corporate governance and requires continuous assessment [1][10].

A process-based assessment approach commonly utilized by information security management frameworks [3][4][5][15] is the maturity assessment model that is adapted from the conceptual model of the capability maturity model (CMM) developed for software process improvement [29]. There is wide acceptance [4][30][31] that to address the requirement for information security assurance through process improvement, the metrics for process-based assessment involve the quality elements defined in the maturity model [29] that consist of consistency, repeatability, predictability of outcomes and continuous optimization. Based these conceptual considerations, it is proposed that:

Proposition 1 (P1)*: The utilization of the quality elements of consistency, repeatability, predictability of outcomes and continuous optimization for process-based security policy assessment will be similar to those quality elements used in the maturity model for continuous process improvement adapted for information security management systems.*

Product-based Assessment: Another driver for security policy assessment is the requirement to ascertain the effectiveness of the security policies as internal controls for achieving and maintaining organizational information security assurance [2][24]. The security policy is based on business and organizational requirements for security risk management [6]. It requires continuous assessment and revision to address evolving risks according to organizational changes [2][11]. The continuous assessment of the security policy ensures practices and procedures within the security policy are coordinated and integrated [2].

In this perspective, the main considerations for product-based assessment are the policy quality elements that address the need for security policies to be aligned with business and/or organizational requirements such as the need for corporate governance or risk management [2][7][8][16]. Other requirements include the need for coordinated and integrated policy structure that is enforced through different levels of internal controls [6] that is implemented according to balanced cost efficiencies [8].

Policy development for information security takes on concepts of strategic planning by way of objective setting and coming up with the program of projects to be undertaken according to the set business objectives. This apparent similarity where it is defined that the security policy contains a layered structure set of sub-policies and procedural implementation that need to be reviewed and assessed may be undertaken in the same manner as that of a corporate strategy or policy and its related program plan of business initiatives.

From this discussion, it may be considered that the development and management of the security policy is a strategic planning process derived from other corporate-level business policy requirements. It is then proposed that:

Proposition 2 (P2)*: The utilization of the quality elements of contextual business alignment, integrated policy structure and cost-efficiencies for product-based security policy assessment will be similar to those quality elements used in the assessment of strategic business policy*.

In the next section, the security assessment methods are evaluated based on propositions ***P1*** and ***P2***.

3. COMPARISON OF SECURITY ASSESSMENT APPROACHES IN THE CONTEXT OF SECURITY POLICY ASSESSMENT

Information security assessments are required to maintain organizational security assurance. Although vast majority of organizations conduct security audits, the tools and methods of assessment used for security is far from universal. Depending on the business objective for security assessment, assessment methods can be categorized as either traditional checklists of security controls or capability maturity assessment methods that focus on audit of processes.

Traditional Checklist Assessment Method: The tools and methods of assessment used for security is far from

universal. Depending on the business objective for security assessment which is usually for compliance and certification purposes, the traditional methods of assessment involve auditing of security technologies and controls against checklists provided by industry standards and best practices. Checklists define the criteria to be used as evaluation basis for the security properties of IT products and systems [32]. Another kind of assessment criteria checklist may also contain basic categories providing internal controls statements for compliance [3][4][5][15][33]. The checklist approach is usually employed for high-level security audit for purposes of meeting certification against the standard or meeting compliance requirements.

Maturity Assessment Models: The traditional checklist approach has progressed to include elements that define the state of maturity of processes as adopted from the assessment approach of the capability maturity model for developed by the Software Engineering Institute for evaluating software development [29]. The maturity assessment model uses a defined 5-level maturity categorization to assess capability based on process maturity. It utilizes a maturity-level checklist to measure process and productivity of the software development life cycle [34][35]. Adapted for assessing information security compliance through standard checklists of security control statements presented by the best practice standards [4][30][31], the maturity model has also been widely used to evaluate the information security management system within the organization.

Evaluation of Assessment Methods

In evaluating assessment approaches in the context of security policy assessment, the conceptual *Propositions 1* (P1) and *2* (P2) are assumed. The relevant factors used as basis for evaluation are: (1) the domain of assessment which is either process-based or product-based; and (2) the set of quality elements represented as domain metrics according to the domain of assessment.

In Table 1, the traditional checklist type and the maturity assessment methods are evaluated whether each method provides either an assessment checklist or a measurement and metrics methodology or both. A check indicates the method provides a means to assess the quality element requirement by providing either a checklist or a measurement methodology (including a metrics development process) or both. A cross means the method does not provide either the assessment checklist or the measurement methodology or both.

Based on this presentation, it is shown that the traditional checklist methods concentrate on assessment against controls defined by the prescribed checklist. It is for this reason that such checklists are used mainly in the conduct of a security audit to assess the extent of security compliance against a prescribed standard. However, the assessment based on predefined controls list does not necessarily reflect the security posture of the organization [10]. Another limitation is that the checklist type of assessment does not define levels of maturity by which an organization can assess itself thus leaving a gap by which to base improvement [36]. The lack of a progressive assessment scheme in traditional assessment methods presents a challenge to the organization in implementing an improvement approach to escalate to a higher level of maturity pertinent to their organizational policy processes, much less their policies structures.

Domain of assessment	Quality elements (domain metric)	Traditional checklist assessment methods		Capability maturity assessment methods	
		checklist	method of measurement and metrics	checklist	method of measurement and metrics
Process-based	***P1***				
	Consistency	✖	✖	✓	✖
	Repeatability	✖	✖	✓	✖
	Predictability of outcomes	✖	✖	✓	✖
	Continuous optimization	✖	✖	✓	✖
Product-based	***P2***				
	Business alignment	✓	✖	✖	✖
	Integrated policy structure	✓	✖	✖	✖
	Cost efficiency	✓	✖	✖	✖

Table 1 Evaluation of Assessment Methods Matrix

On the other hand, it is also shown that maturity assessment approaches concentrate attention on the evaluation of the process itself. This results in the oversight of assessing the resultant policy product that the process is producing. Solely utilizing the maturity assessment methods will not provide sufficient assessment results to provide an understanding of the effectiveness of the security policies based on business alignment and cost efficiency.

The utilization of any single assessment method provides assessment results relative to only those quality elements that comprise the domain used in the assessment. This linear assessment presents inherent disadvantages as assessment is not based on the whole context of policy development that should be multi-dimensional [12]. For example, using process-based assessment alone will provide assessment results relating to the policy development process and not necessarily relevant to policy effectiveness. Alternatively, even if the assessment methods are undertaken in combination, the utilization of the unsynchronized assessment methods presents problems in metric correlation that may consequently lead to conflicting and therefore unreliable results.

4. METRICS DEVELOPMENT FOR ENTERPRISE INFORMATION SECURITY POLICY ASSESSMENT

The conceptual similarities between software engineering and information security have encouraged the adoption and adaptation of software management processes and assessment models in information security.

The Goal-Question-Metric (GQM) was developed as a measurement approach for software development [37]. The method is based upon the assumption that meaningful measurement should be based on pre-defined goals for the assessment. The GQM approach was originally defined for evaluating software defects in government projects [38]. The result of the application of the GQM is a measurement system targeting a defined set of issues and rules for interpreting measurement data in three levels [13] as shown in Figure 1:

1) Conceptual level (GOAL) - a goal is defined for objects of measurement which are products, processes and resources.

2) Operational level (QUESTION) - a set of questions is developed to characterize the manner of assessment of a goal.

3) Quantitative level (METRIC) - a set of measurement data generated to answer each question in a quantitative way.

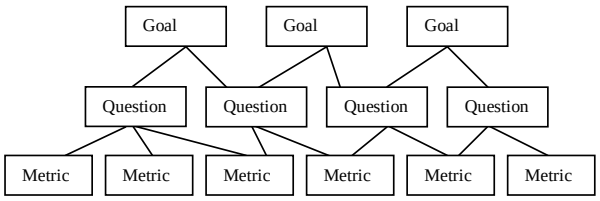

Figure 1 The Goal-Question-Metric Method
(Source: Adopted from Basili et al, 1994)

In addressing the lack of a metrics development approach in security assessment methods, the GQM is considered in this paper. There are however differences between software engineering and information security that present issues and disadvantages if these are not considered in formulating such adaptations. One such major difference is that unlike software development which is a project-based undertaking driven by a business requirement for the delivery of a software product, information security is based on an ongoing business requirement for corporate governance that is defined by the security policy. The security policy is recognized as a strategic policy that may be developed and managed according to the strategic alignment contexts of corporate risk management [19] and strategic management [20]. Thus, metric development for security policy requires an expansion to the GQM approach to allow for the consideration of the contextual alignment. This is presented in the next section.

Enterprise Information Security Policy Assessment: An Extended GQM Approach

Existing literature provides several varying security policy theories [39] [11] [6] [40][19] that present different perspectives and approaches on the development and management of security policies. Recent security policy management theories attempt to provide more focus on the requirement for alignment with corporate business objectives for risk management [19], IT planning [41] and strategic planning [20]. These approaches are based on the business planning and information systems planning integration approaches of previous research studies [42][43][44][45]. As a major consideration for security policy is its alignment with business objectives, assessment of the security policy should involve the degree of alignment between the security policy and the strategic business context for which the policy was developed. Based on this correlation between the policy alignment context and the metric development, the following hypothesis is proposed:

Hypothesis 1 (H1)*: Establishing the alignment context for security policy management positively affects the alignment of the top-down definition of goals, questions and metrics with the business requirements.*

The GQM [37] developed for software does not present an element for policy context consideration. To address this limitation and allow for the adoption of hypothesis 1 ***H1***, it is then proposed that the GQM approach is expanded as presented in Figure 2. The steps involved in the extended approach are as follows:

Step 1: Establish policy alignment context - alignment perspectives for developing and managing security policy may be based on risk management [19] [Corpuz and Barnes 2010], IT planning [41] or strategic management [20] [Corpuz 2011]. This step will align the assessment goals for the security policy, whether it is addressing corporate risks or providing corporate support as a strategic business policy.

Step 2: Define goals - goals for security policy pertain to the three objects of measurement for the security policy: (1) the security policy product; (2) the security development process; and (3) the policy resources used in implementation.

Step 3: Develop questions - questions characterize the object of measurement (product, process, resource) with respect to a quality element. Questions can be generated using the quality elements (domain metrics) for product-based and process-based assessment in Table 1 of Section 3:

Process-based: quality elements of consistency, repeatability, predictability of outcomes, continuous optimization.

Product-based: quality elements of business alignment, integrated policy structure, cost efficiencies.

Resource-based: quality element of cost efficiencies

Step 4: Define metric - generate the set of data according to the defined metric as quantitative responses to the questions.

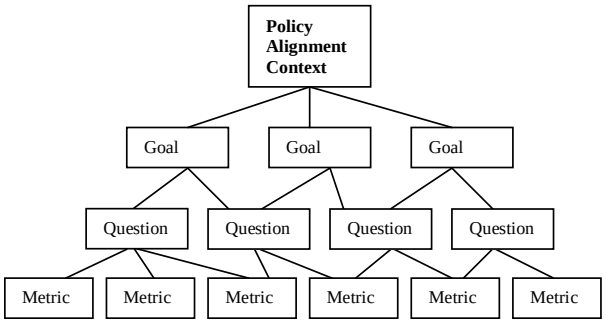

Figure 2 Enterprise Information Security Policy Assessment: An Extended GQM approach

5. A CASE EXAMPLE

An organization requiring an update to its security policy will conduct security policy assessment based on the organizational context of corporate risk management. With the assumption that enterprise information security is aligned with the corporate risk management, the following measurement approach based on the proposed extended GQM approach will yield the following as shown in Figure 3.

Step 1: Establish policy alignment context - policy alignment context is with corporate risk policy

Step 2: Define goals - goals include:

(1) security policy and policy structure should be aligned with corporate risk policy.

(2) security development process should be generate business improvement.

(3) the resources used in the security policy process should be optimally utilized within planned budget allocation.

Step 3: Develop questions - questions characterizing the policy product, process and resource with respect to the defined quality elements:

Process-based: Is policy development process repeatable and standardized to facilitate ongoing implementation and business improvement?

Product-based: Is policy aligned with risk management requirements for security controls?

Resource-based: Is policy implementation using resources in the optimum way?

Step 4: Define metric - the set of data as quantitative responses to the questions:

Process-based: Generate user compliance to procedural policies in percentage.

Product-based: Generate number of mitigated risks compared to targeted risk controls.

Resource-based: Generate cost savings in policy development through avoidance of rework in man-hours.

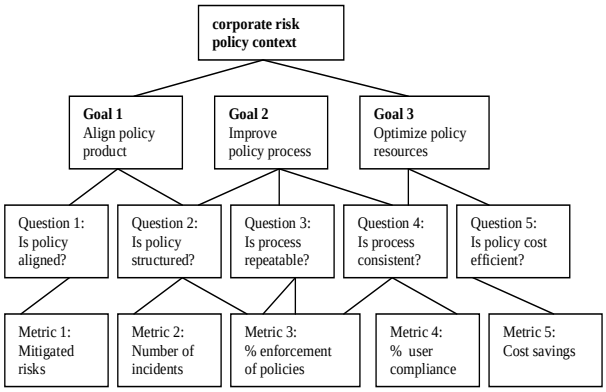

Figure 3 Case example: A GQM Metric Matrix with Policy Alignment Context Consideration

6. CONCLUSION

The management of enterprise information security policy is a strategic management activity that can be presented as an integrally aligned undertaking with corporate risk management and strategic planning. This allows for strategic management tools and methods to be adapted for security policy development and assessment. Further, security policy assessment can also adapt software development tools and process for assessment and metrics development. These conceptual adaptations for security policy management fill the gap and address limitations in existing security management approaches. Such gaps include the need for policy assessment approach and metrics development.

This paper provides a method selection for policy assessment from the current security assessment approaches through a matrix comprised of quality elements provided by the traditional assessment methods. In presenting and addressing limitations in utilizing the current approaches, the paper proposes an extended GQM approach to facilitate goal-based multi-dimensional assessment approach and a method to develop measurement metrics. By providing an example case scenario, it is briefly shown that the proposed framework addresses the requirement for developing assessment metrics and allows for concurrent process-based and product-based assessment. Metrics that can be developed include aspects such as the success rate of enforcement and the efficiency and effectiveness of the policies to address risk mitigation requirements.

Recommendations for further research activities include the conduct of empirical research to validate the propositions and the practical application of the proposed assessment approach in case studies to provide opportunities to note further enhancements to the approach.

7. REFERENCES

[1] V. LeVeque, **Information Security A Strategic Approach**, John Wiley and Sons Ltd, 2006.

[2] Organization for Economic Co-operation and Development OECD, **OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security**, OECD , 2002.

[3] International Standards Organization ISO/IEC, **ISO/IEC 27001: Information technology – Security techniques – Information security management systems – Requirements**, International Standards Organization, 2005.

[4] IT Governance Institute ITGI, COBIT 4.0 **Control Objectives Management Guidelines Maturity Models**, ITGI, 2005.

[5] M. Swanson and B. Guttman, **NIST Generally Accepted Principles and Practices for Securing Information Technology Systems Special Publication 800-14,** National Institute of Standards and Technology, 1996.

[6] R. Baskerville and M. Siponen, "An Information Security Meta-Policy for Emergent Organizations", **Logistics Information Management**, Vol. 15 No.5/6, 2002, pp. 337-346

[7] W. Caelli, **Information Security Handbook**. Macmillan Publishers Ltd, 1991.

[8] B. von Solms and R. von Solms, The 10 deadly sins of information security management, **Computers and Security**, 2004, Vol. 23, pp. 371-376.

[9] E. Humphreys, "Information Security Management Standards: Compliance, governance and risk management", **Information Security Technical Report**, Vol. 13, 2008, pp.247-255.

[10] K. Hone and J.H.P. Eloff, "Information Security Policy – What Do International Information Security Standards Say", **Computers and Security**, Vol. 21, Issue 5, 2002, pp. 402-409.

[11] J. Rees, S. Bandyopadhyay and E. Spafford, PFIRES: A Policy Framework for Information Security. **Communications of the ACM,** Vol. 45. No. 7, 2003, pp. 101-106.

[12] M. Corpuz, "Limitations of the Information Security Management System Assessment Approaches in the Context of Information Security Policy Assessment" (Extended Abstract). **Proceedings of the Symposium on Risk Management and Cyber-Informatics (RMCI 2010) of the 14th World Multiconference on Systemics, Cybernetics and Informatics** Vol 4 (Post Conference Edition), 2010, pp.148-150,Orlando USA, 2010.

[13] V. R. Basili, G. Caldiera, R.H. Rombach, "The Goal Question Metric Approach", **Encyclopedia of Software Engineering** (Marciniak, J.J., editor), Volume 1, John Wiley & Sons, 1994, pp. 578-583.

[14] G. Oyomno, **"Towards a Framework for Assessing the Maturity of Government Capabilities for E-Government".** Southern African Journal of Information and Communication (SAJIC), The Edge Institute / Research ICT Africa, Braamfontein, ZA. University of the Witwatersrand. Johannesburg. 2003.

[15] J. Cazemier, P. Overbeek, L. Peters, **IT Infrastructure Library Best Practice for Security Management**. Office of Government Commerce, Crown Copyright, 1999.

[16] A. Calder, and S. Watkins, *"IT Governance: Data Security & BS7799/ISO 17799. A Manager's Guide to Effective Information Security"*, Kogan Page, 2002.

[17] Standards Australia, **Australian Standard. AS 8015-2005: Corporate Governance of Information and Communication Technology**, Standards Australia, 2005.

[18] Organization for Economic Co-operation and Development OECD, **Working Party on Information Security and Privacy. Summary of Responses to the Survey on the Implementation of the OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security**, OECD, 2004.

[19] M. Corpuz and P. Barnes, "Integrating Information Security Policy Management with Corporate Risk Management for Strategic Alignment", **Proceedings of the 14th World Multi-Conference on Systems, Cybernetics and Informatics Proceedings**, Vol 4, 2010, Florida USA, pp.337-342.

[20] M. Corpuz, "The Enterprise Information Security Policy as a Strategic Business Policy within the Corporate Strategic Plan", **Proceedings of the 15th World Multi-Conference on Systems, Cybernetics and Informatics Proceedings**, 2011, Florida USA.

[21] A. McCullagh, "Management Responsibility in Protecting Information Assets: An Australian Perspective", Peer-Reviewed Journal on the Internet. Accessed on December 2010 http://www.firstmonday.org/issues/issue7_7/mccullagh/index.html. 2005.

[22] P. Fites, M. Kratz and A. Brebner, "Control and Security of Computer Information Systems", Computer Science Press, 1989.

[23] B. von Solms, "Corporate Governance and Information Security", **Computers & Security**, 20(3), 2001, pp215-218.

[24] M. Devargas, "The Total Quality Management Approach to IT Security", NCC Balckwell. 1995.

[25] V. Basili, G. Caldiera and H. D. Romback, "Meaurement", Accessed online on February 2011, http://www.cs.umd.edu/~basili/publications/technical/T87.pdf

[26] B. von Solms, "Information Security- A Multidimensional Discipline", **Computers & Security**, 20, 2001, pp504-508.

[27] J. Kay, P. McKiernan and D. Faulkner, "The History of Strategy and Some Thoughts About the Future", **The Oxford Handbook of Strategy** (Eds: D. Faulkner and A. Campbell), Oxford University Press, 2003, pp27-52.

[28] T. Wheelen and J. Hunger, **Strategic Management and Business Policy: Concepts and Cases**, New Jersey: Pearson Prentice and Hall Pub., 2008.

[29] M. Paulk, B. Curtis, M. Chrissis and C. Weber. "Capability Maturity Model for Software Version 1.1", **Technical Report CMU/SEI-93-177**, Software Engineering Institute, 1993.

[30] National Institute of Standards and Technology, "Federal Information Technology Security Assessment Framework", **Security, Privacy and Critical Infrastructure Committee,** United States Department of Commerce, United States of America, 2000.

[31] International Standard Organization, IEC, "ISO/IEC 21827: Information technology – Systems Security Engineering – Capability Maturity Model (SSE-CMM)", **ISO/IEC**, 2002.

[32] Australian Standard, "Information technology – Security techniques – Evaluation criteria for IT security Part 1: Introduction and general model", **AS ISO/IEC 15408.1-2004**, Standards Australia, 2004.

[33] Computer Security Institute, "IPAK: Information Protection Assessment Kit", **IPAK**, Computer Security Institute Publication, 2003.

[34] R. Pressman, "Software Engineering", **Software Engineering Volume 1: The Development Process, Third Edition,** IEEE Computer Society, 2005.

[35] R. Linger, M. Paulk and C. Trammell, "Cleanroom Software Engineering Implementation of the Capability Maturity Model for Software", **CMU/SEI Technical Report**, Software Engineering Institute, 1996.

[36] M. Siponen, Towards Maturity of Information Security Maturity Criteria: Six Lessons Learned from Software Maturity Criteria", **Information Management and Computer Security Vol. 10 (5)**, 2002, pp. 210-224.

[37] V. Basili and D. Rombach, "The TAME Project: Towards Improvement-Oriented Software Environments", **IEEE Transactions on Software Engineering**, Vol. SE-14, 1988.

[38] V. Basili, "The Experimental Paradigm in Software Engineering. Experimental Software Engineering Issues: Critical Assessment and Future Directives", **Proceedings of Dagstuhl-Workshop** (Lecture Notes in Computer Software). Springer-Verlag, 1993.

[39] M.E. Kabay, **The NCSA Guide to Enterprise Security**, McGraw-Hill, New York, 1996.

[40] M. Siponen and J. Iivari, "Six Design Theories for IS Security Policies and Guidelines", **Journal of the Association for Information Systems 7(7)**, 2006, pp 445-72.

[41] N. F. Doherty and H. Fulford, "Aligning the Information Security Policy with the Strategic Information Systems Plan", **Computers and Security** Vol. 25, 2006, pp. 55-63.

[42] W. R. King, "Strategic Planning for Management Innformation Systems", **MIS Quarterly**, Vol 2 (1), 1978, pp. 27-37.

[43] W. R. King and R. W. Zmud, "Managing Information Systems: Policy Planning, Strategic Planning and Operational Planning, **Proceedings of the Second International Conference on Information Systems**, Boston, 1981.

[44] N. Goldsmith, "Linking IT Planning to Business Strategy", **Long Range Planning**, Vol. 24, No. 6, 1991, pp. 67-77.

[45] A.L. Lederer and V. Gardiner, "Strategic information systems planning: The Method/1 approach. **Information Systems Management**, Vol. 9(3), 1992, pp. 13-20.