# A Paradigmatic Analysis of Conventional Approaches for Developing and Managing Secure IS

*Implications for research and practice*

MIKKO T. SIPONEN
*University of Oulu, Department of Information ProcessingScience, Linnanmaa, P.O.BOX 3000, Oulu, FINLAND. E-mail:Mikko.T.Siponen@oulu.fi*

Key words: Information Security Management

Abstract: Because the methods of development for Information Systems (IS) do not pay attention to security aspects, several information systems (ISS) security methods have been presented. This paper will analyze traditional/conventional approaches, namely normative standards (e.g. checklists, management and evaluation standards), formal methods, common sense principles and risk management. These approaches will be analyzed in the light of I) the research objectives; II) the organizational role of IS security; III) research approaches used; IV) applicability; and V) a conceptual meta-model for IS. The contribution of the paper is twofold. First the analysis sheds new light on the underlying foundations of the conventional approaches. Second, the analysis suggests several implications for researchers and practitioners.

## 1. INTRODUCTION

Despite the recognized relevance of IS security (e.g. Baskerville, 1992; Straub & Welke, 1998), IS security design aspects are neglected in IS development methods (Baskerville, 1992; Dhillon & Backhouse, 2001). The information security community at large has gotten stuck in technical small-scale questions (e.g. Dhillon & Backhouse, 2001; Thomas & Sandhu, 1994) and the thesis propounding that the key issue in development is “‘formalization” (e.g. Anderson, 1993; Barnes, 1998). To overcome this weakness, several methods for the development of secure ISs, from checklists to different approaches based on IS or software development methods, are proposed (Baskerville, 1993; Dhillon & Backhouse, 2001; Siponen, 2001a). It is interesting to note that the naturalistic approaches, such as normative standards, risk management and formal methods, have survived well. Checklists (herein classified as normative standards) and risk management approaches have been widely used (Baskerville, 1992; Fitzgerald, 1993) and different normative standards such as Generally Accepted System Security Principles (GASP, 1999), SSE-CMM (1999a; 1999b) and BS 7799 (1993) have been recently announced. Furthermore, different normative standards are highly rated by many security experts (e.g. Fitzgerald, 1995; von Solms, 1997; 1998; 1999). Additionally, the use of formal methods have been advocated by the Computer Security community (e.g. Anderson, 1993; Barnes, 1998). Recently, an interest to scrutinize the theoretical foundations of the alternative approaches for designing and managing IS security have been increased. Consequently, Baskerville (1993), Parker (1998) and Siponen (2001b) have took a critical look at checklists and security management standards. Dhillon & Backhouse (2001) and Dhillon (1997) have analyzed methods for developing secure IS's in the light of Burrell & Morgan. Siponen (2001a) have analyzed the recent (non-conventional) approaches. This paper continues these research efforts. The conventional approaches will be analyzed from the viewpoints of I) the research objectives; II) the organizational role of IS security; III) research approaches used; IV) applicability; and V) a conceptual meta-model for IS.

Conceptual analysis in terms of Järvinen (1997) is used as the research approach of this paper,

The rest of this paper is organized as follows. In the second section, the framework for analysis is presented. In the third section normative standards are analyzed. In the fourth section, the risk management approach is considered. Fifth section analyzes formal methods. The sixth section discusses the implications of this study. In the seventh section, the key issues are summarized.

## 2. THE FRAMEWORK FOR ANALYSIS

The following framework will be used to carry out the analysis.

*Table 1.* The viewpoints/tools of the analysis

| Viewpoints | Reasons |
|---|---|
| 1) The research objectives | 1) To perceive what is the goal of research |
| *2)* Organizational role of Information Systems Security | 2) To see what is the organizational role of IS security development |

| Viewpoints | Reasons |
|---|---|
| 3) Research approaches used | 3) To see what research approaches are used and preferred to a) develop IS security methods; b) validate the solutions |
| 4) Applicability into IS and software development | 4) To see whether the security methods can be integrated to IS or software development |
| 5) A meta-model for IS | 5) What aspects of IS do the contributions cover? |

These viewpoints are discussed next.

*The research objectives*

Based on the classification by Chua (1986), the objective of scientists can be divided into 1) means-end oriented; 2) interpretive; 3) critical - though we shall herein simplify these concepts. A means-end oriented view holds that the aim of research is to produce knowledge for achieving certain concrete goals or ends. For example, development of a new algorithm is an example of means-oriented research. For Chua, the means "to enrich people's understanding of the meaning of their actions" (Chua, 1986 p. 615). The importance of interpretive research is widely accepted in social sciences – and IS science have close connections to social sciences since information systems are social systems (Hirschheim, 1985). Hence, interpretive research seems to be relevant for IS (e.g. Hirschheim, 1985; Walsham, 1996; Galliers & Swan, 1997; Klein & Myers, 1999). The goal of critical research is to point out the weaknesses of the existing theories/practices.

*Organizational roles of lnformation Systems Security*

Three organizational roles of Information Systems (Security) can be categorized into technical, socio-technical and social roles (Iivari & Kerola, 1983; Iivari & Hirschheim, 1996). According to the technical view, the emphasis of IS development lies in technical matters, and the possible social implications of IS development are at best afterthoughts. Social schools emphasize the development of organizational systems (before technical matters); and the sociotechical view contends that technical and organizational systems are equally important (Iivari & Hirschheim, 1996).

*Research approaches*

The research approach viewpoint indicates how the development approaches themselves are developed and validated. For example, a question such as "are approaches validated empirically or conceptually?" can be answered by indicating the used research approaches. The classification of research methods is adapted from Järvinen (1997). According to our knowledge, there are other classifications of research approaches and methods including Jenkins (1985); Galliers & Land (1987); Goubil-

Gambrell (1991); Iivari (1991b); Nunamaker et al. (1991); Stohr & Konsynski (1992); March & Smith (1995) and Wynekoop & Russo (1997). The one by Järvinen (1997) was chosen since it is systematic and holistic.

*Applicability into IS development*

The problem of developmental duality means that the normal system development and security development are separate activities having conflicting requirements among other weakness (Baskerville, 1992). Due to such conflicts, separate security methods (i.e. those that cannot be integrated into normal IS development) should be eliminated altogether (Baskerville, 1993 p. 410). The problem of developmental duality can be retraced to Ockham's razor "Plurality should not be assumed without necessity" (Baskerville, 1988 p. 93). Ockham's razor briefly means: keep it simple. In other words, in the case of compelling theories, for example, the preference should be given to the simplest theory.

The most extensive formulation of Ockham's (1990) razor is also worthwhile to note: "Nulla pluralitas est ponenda nisi per rationem vel experientiam vel auctoritatem illius, qui non potest falli net errare, potest convinci". This means that no plurality should be accepted unless it can be proved (i) by reason, or (ii) by experience, or (iii) by some infallible authority (Ockham, 1990). Let us apply this version of Ockham's razor/eraser to IS security methods in a pragmatic sense. Without IS it is difficult to see something called IS security. To have ISS, it seems rational that there is something called IS (we, however, do not thereby claim in ontological argument that IS exits in the fundamental ontological sense). If there were no IS, would there be any (pragmatic) need for ISS? IS is a human construction. IS does not rain down from sky - so to have an IS, we need to develop one. So to develop IS we need to use a method (whether the methods is formal, semi-formal, or totally informal). Hence, to develop an IS we are likely to adopt a method (remember our loose use of method). Thus, it generally seems that the "existence" of IS requires a method, of which result, the IS is developed. So, the "existence" of an IS method (or development process) is quite necessary. By contrast, an IS exists without any security development - though it would perhaps be insecure (and this may cause certain complications). In that respect, security method/development is, in a pragmatic sense - dependent upon the existence of IS (and IS method, by which the IS was built). In turn, IS security is not a necessary prerequisite for the development of IS (though security may be important for carrying out the operations of IS successfully) - the IS can exist (as a human construction) without security development. In other words, IS security is ontologically dependent (using term by Niiniluoto, 1999 p. 27) on IS (ISS could not exists without IS existing). When separated security methods are applied to existing IS, the plurality comes into play (as described by Baskerville (1988; 1992)): security development may have its own requirements (that are conflicting with IS development), etc. Therefore, we can conclude that in a general sense the plurality should be avoided and we showed that the source of plurality was the separate ISS method, since generally an IS development method is more a prerequisite for IS than ISS method. Corollary, Ockham's razor insists that stand-alone security method should be eliminated.

*Meta-model for IS*

The meta-model used is one by Iivari (1989). It is based on a commonly agreed separation between three levels of modeling/abstraction for an IS (Iivari & Koskela, 1987; Iivari, 1989; Lyytinen, 1987): 1. The organizational level, which defines the organizational role and context of the IS. 2; The conceptual level, which defines an implementation-independent specification for the IS.3; The technical level, which defines the technical implementation for the IS. Originally (Iivari, 1989), the levels are in order of abstraction. Hence, for example, the conceptual level can be seen as an abstraction of the organizational level. Since the meta-model is based on the commonly agreed levels of IS, it shows which aspects of information systems are covered by different methods. In other words, it provides a framework for analyzing the breadth of each developmental approach. However, it does not pay attention to the relevance of the content (including processes, notations, etc) of the approaches. For example, the meta-model, per se, does not give much information about such issues as ease of use, tool support, or conflicts within the processes, etc.

## 3. NORMATIVE STANDARDS

Normative standards include checklists (AFIPS, 1979; Wood et al., 1987; Cooper, 1989; Custance, 1996; Moulton & Moulton, 1996), management standards (e.g. Code of Practice/BS 7799, 1993; CobiT, 1995; GASSP, 1999; IT Protection Manual, 1996) and non-technical evaluation and maturity criteria (see e.g. Chokhani, 1992; Abrams & Podell, 1995).

The evaluation, management and maturity standards can also be included into a category of development methods since they strongly guide development (e.g. by improving processes or products). As they all propose norms for developing or managing secure ISs they can be classified as normative standards (Siponen, 2001b). Many of the evaluation criteria such as TCSEC/Orange Book and Common Criteria are inadequate from an

IS/management/organizational perspective since they focus on technical or implementation level issues.

The security maturity standards such as the System Security Engineering Capability Maturity Model (henceforth SSE-CMM) differs from traditional checklists (and similar standards) in two respects. First, SSE-CMM has a non-organizational/public dimension, as well. This means that SSE-CMM - ideally - shows the security level of organization for partners and customer, for instance (SSE-CMM, 1998b). However, from the viewpoint of the organization, this means that the standard is more seriously adapted to guide development. Secondly, SSE-CMM has a concept of process areas (e.g. see Ferraiolo & Sachs, 1996) that is similar to "second generation mechanistic methods" (classified by Baskerville, 1993) that pays attention to the organizational differences. Other maturity approaches include Stacey’s (1996) approach reflecting on CMM and Murine's & Carpenter's (1984) SSM that measures system security using software security metrics, which is based on software quality metrics (SQM). According to our knowledge, they have not gotten common recognition.

Another recent effort to build widely accepted evaluation criteria is the Common Criteria (CC), which is focused on products and processes. The validation of CC is based on expert validation. One of the important difference between SSE-CMM and CC is that CC does not take into account non-technical aspects (Overbeek, 1995).

*The research objective*

The research objective behind the checklist is means-oriented. The aim is secure information systems by implementing a certain set of solutions.

*The organizational role of IS security*

The organizational role of Information Systems security is technical. The primary focus of the secure IS developed rests on technical issues. The organizational structures and social implications come as afterthoughts.

*The research approaches and the meta-model*

According to our knowledge, the normative standards are based on authors’ experiences. In that way, we really cannot say that they are developed using a certain research approach. If the authors' observations and results thereof were available, we might be able say that they are based on theory creating or theory testing research (cf. Järvinen, 1997). Checklists/normative standards provide only organizational level support for designing secure IS.

*Applicability in the IS development process*

Checklists do maintain the dualistic development, meaning that security and normal ISD are developed separately, having conflicting requirements, among other weaknesses (Baskerville, 1988; 1992).

## 4. RISK MANAGEMENT TECHNIQUES

Risk management (RM) approaches have been traditionally used in the field of IS after its development in the nuclear arena (Tarr & Kinsman, 1996) and is a de facto topic of non-technical textbooks (e.g. Gollman, 1999; Norman, 1983; Parker, 1998). Several RM approaches have been presented (Wong, 1977; Cooper, 1989; Custance, 1996; Veatc et al., 1995; Moses, 1995; Bennett & Kailay, 1992; Halliday et al. 1996; Lichtenstein, 1996; Freeman et al., 1997; Jung et al. 1999; Spruit & Samwel, 1999). The terms risk analysis/management/assessment are used very differently by different authors, and without muddling through the terminological mess, we hereafter apply the term RM.

*The research objectives*

As for the research objective, RM techniques are both 1) means-end oriented and 2) interpretive. They are clearly means-oriented since the aim of risk management is to provide feasibility justification, as mentioned. There have also been reasons reported for why RM is interpretive. For example, Baskerville (1991b) argues that the role of risk management is interpretive. We understand his view as follows: Baskerville (1991b) seems to acknowledge that RM is inadequate as a means-oriented tool, but that it may be valid as an interpretive method (RM provides clear numbers for managers). Also, Guarro sees that the objective of risk management is interpretive. The aim is of RM is to understand the environment (Guarro, 1987).

*The organizational role of Information Systems*

The organizational roles of IS security are mainly technical. For the RM community (generally speaking), the technical system is the first preference and the issues concerning social systems come second.

*The research approach and Meta-model*

Risk management approaches are based on conceptual analysis. Risk management provides only organizational level support for designing secure IS.

*Applicability in the IS development process*

The risk management approaches maintain the problem of developmental duality: There is no explicit guidance about how RM could be integrated to IS or software development process.

## 5. FORMAL MODEL DEVELOPMENT

Formal model-oriented development (FMD) holds that IS or SW development should be based on formally validated components or carried out by formal methods. Formal refers to use of logic as the reference discipline - preferably hard analytic philosophy (see the philosophical assumptions) – by which the security of the solutions can be validated, i.e. meet certain requirements. This appears to be held by a majority of computer science security researchers: the crucial problem behind insecure systems is the lack, or wrongful use or implementation, of formal development (e.g. O'Leary et al., 1990; Parnas et al. 1990 p. 647; Anderson, 1993; Freeman & Neely, 1993; Williams & Abrams, 1995; Barnes, 1998; McDermott & Fox, 1999).

*The research objectives*

The research objective is means-oriented - to provide a tool for reliable and secure implementation.

*The organizational role of Information Systems*

The view of the organizational role of IS is technical. The design objective lies in technical systems. Poor technical quality is behind the security problems, because the most important condition for achieving secure systems is technical quality.

*The research approach and Meta-model*

As can be seen, the favored research approach is mathematical modeling. All "modeling" support is concentrated on an technical level in terms of Iivari's meta-model (Iivari, 1989). Formal model approach does not propose any organizational or conceptual modeling means.

*Applicability into IS Development Process*

FMD maintains the duality problem. Suggestions for the integration of security and normal ISD/SW development have been proposed, including Zhou et al. (1999). These are, however, mainly concentrated on implementation (some even more specified) issues, ignoring logical level issues (e.g. modeling). According to Evans & Welling (1999), formal methods are even rejected by many practitioners because they are regarded to be too lower level. The integration of security development and normal ISD is also difficult due to differences between notation and approaches (Evans & Welling, 1999). Normal IS development is rarely carried out in a formal manner.

## 6. COMMON SENSE PRINCIPLES

Common sense principles (CSP) refer to principles (i.e. loose guidelines, but not as holistic guidelines as checklists) that are "validated" or reasoned by the authors' own experiences. As many of them are accepted (e.g. Garfinkel & Spafford, 1997; Parker, 1998 p. 329-330; Summers, 1997 p. 250-252; Zurko & Simon, 1996), though these principles are based on a less disciplined development process (not validated in a scientific manner), we may call them as CSP. The difference between the "principles" and checklists and other normative standards is that the "principles" 1) are more abstract than checklists; and 2) are more guiding and not argued to be universally valid, while checklist are argued to be, somewhat universally valid. There are several other or modified CSP’s, such as proposed by Fisher (1984), Essinger (1992), Fites & Kratz (1993), Finne (1995), OECD (1996), Sherwood (1996), Coyle et al. (1997), Parker (1998) and Nitzberg (1999). There are no studies testing the principles in practice, for example. As the principles are very abstract and not systematic, they do not per se form a process that could guide development.

*The research objective*

The CSPs are generally means-oriented. The research objective is to produce guidance, by the help of which the goal, i.e. more secure systems, can be achieved.

*The organizational role of ISS*

Generally, the organizational roles of IS security of the different principles are technical, though there are exceptions, such as Angel (1993), who seems to hold a social view.

*The research approach and Meta-model*

We did not find any research approaches that were used to develop the principles. It is possible that empirical research, particularly theory testing and theory creating, as well as conceptual analysis, could be used to develop these principles (and perhaps are used unconsciously, and therefore are not reported). In terms of Iivari's (1989) meta-model for IS, these principles provide only organizational level (functional abstraction since they may be understood as work procedures) support for security development.

*Applicability in IS development*

The principles are faced with the problem of developmental duality. They do not propose any means by which these principles can be integrated to normal IS development. Moreover, principles such as separation of duty may often conflict with information systems normal requirements.

## 7. DISCUSSION AND IMPLICATIONS FOR RESEARCH AND PRACTICE

The implications summarized in Table 2.

*Table 2.* Implications in the light of different viewpoints.

| Viewpoints | Findings | Implications |
|---|---|---|
| Research objectives | Mainly means-oriented | Alternative approaches are needed |
| Organizational role of IS security | Mainly technical | Alternative approaches (more socio-technical, social) are needed |
| Research approaches | The conceptual analysis was the research approach most used | Additional empirical studies are needed |
| Applicability | Conventional approaches cannot be integrated into IS or software development | Conventional approaches cannot be integrated into IS development. More guidance is needed about how the approaches could be integrated into IS development |
| Meta-model for IS | Approaches were not comprehensive: they give only organizational level support | Given that all levels of IS are relevant to the model, new approaches that can provide comprehensive support are needed |

These implications will be discussed next.

*Research objectives*: As for conventional methods, the most commonly held view about the objectives of that IS security research is means-oriented. It is widely suggested that due to the social dimensions of IS, alternative approaches, particularly the interpretive approach, are needed (Klein & Lyytinen, 1985; Hirschheim, 1985; Walsham, 1996; Galliers & Swan, 1997; Klein & Myers, 1999). It is postulated that critical approaches are needed as well. The development cannot be based on "blind" approaches - the risks are far too high, for our assumptions may be proven wrong in the final analysis. Therefore, critique plays an essential role by keeping us on our toes, and forcing us to prove our ideas.

The most commonly held *organizational role of IS security* was the technical view. This results in practitioners having only technical and a few socio-technical approaches available from which they can choose an IS security development method. Recently, many studies (e.g. Dhillon & Backhouse, 2000; Dhillon & Backhouse, 2001; Baskerville, 1988; Dhillon, 1997) have strongly advocated the relevance of the socio-technical role. They mainly argue that a technical "engineering" approach is too technical in an organization since an organization is a social institution.

*Research approaches used.* The conceptual analysis/intuition is used to develop all the conventional approaches excluding FMD, which uses mathematical modeling. Disciplined empirical studies from a wide cross-section - 1) in which neither the research process nor the results are secret and 2) all possible variables are considered - as well as real conceptual analysis (which is not based on intuitions and which takes the relevant research and objections into account) are needed.

*Applicability into IS/software development process*: Conventional approaches cannot be integrated into IS development. Given that the development and use of conventional approaches is still desired, it is suggested that more guidance about the integration of the conventional approaches into IS development is needed.

*The meta-model for IS*: The conventional ISS approaches only cover the organizational level, except for FMD, which provides support on technical levels, as well. As a result, more holistic approaches that cover all levels of IS (organizational, conceptual, technical) are needed.

## 8. CONCLUSIONS

Conventional approaches for secure IS development were explicated: checklists/normative standards, common sense principles and formal development. Whese approaches were analyzed from the viewpoints of I) the research objectives; II) the organizational role of IS security; III) research approaches used; IV) applicability; and V) a conceptual meta-model for IS.

The dominating research objective is means-oriented. The research approaches used range from mathematical modeling (formal methods) to conceptual analysis (risk management). Risk management techniques have traditionally been means-end oriented, but recently their interpretive roles have been recognized. Common sense principles and normative are not based on any research approach/method. The dominating organizational role of IS security is technical (normative standards, risk management, formal methods and most common sense principles).

The conventional approaches are not applicable to IS or software development, resulting the problem of developmental duality.

As for the meta-model for IS, the approaches are within organizational (standards, risk management, common sense principles) and technical contexts (formal development).

## 9. REFERENCES

Abadi, M. & Needham, R., (1994), Prudent Engineering Practice for Cryptographic Protocols. Proceedings of the 1994 IEEE Symposium on Research in Security and privacy.

Abrams, M.D. & Bailey, D., (1995), Abstraction and Refinement of Layered Security Policy. In: Information Security - An integrated Collection of Essays. Edited by M. D. Abrams, S. Jajodia & H. J. Podell. IEEE Computer Society Press, Los Alamitos, California, USA.

Abrams, M.D., & Podell, H.J., (1995), Evaluation issues. In: Information Security - An Integrated Collection of Essays, Edited by M. D. Abrams, S. Jajodia & H. J. Podell, IEEE Computer Society Press, CA, USA.

Angel, I., (1993), Computer Security in these uncertain times: the need for a new approach. Proceedings of the 10th International Conference on Computer Security, Audit and Control (CompSec), London, October.

Anderson, R., (1993), Why Cryptosystems Fail. Communication of the ACM, November, vol. 37, no. 11., pp. 32-44.

Barnes, B.H., (1998), Computer security research: a British perspective. IEEE Software. Volume 15, no 5, Sept.-Oct. Pp. 30 -33.

Baskerville, R., (1988), Designing Information Systems Security. John Wiley Information Systems Series.

Baskerville, R., (1991a), Risk Analysis: An Interpretative Feasibility Tool In Justifying Information Systems Security. European Journal of Information Systems Vol. 1, Issue 2, pp. 121-130.

Baskerville, R., (1991b), Risk Analysis As A Source of Professional Knowledge. Vol. 10, Issue 8, pp. 749-764.

Baskerville, R., (1992), The Developmental Duality of Information Systems Security. Journal of Management Systems. Vol. 4, no. 1, pp. 1-12.

Baskerville, R., (1993), Information Systems Security Design Methods: Implications for Information Systems Development. Computing Surveys 25, (4) December, pp. 375-414.

Bennett, S. P., & Kailay, M. P., (1992), An application of qualitative risk analysis to computer security for the commercial sector. Proceedings of the Eighth ACM Annual Computer Security Applications conference.

Blakley, B, Kienze, D.M., (1997), Some Weaknesses of the TCB model. Proceedings of the 1997 IEEE Symposium on Security and Privacy. IEEE Computer Society Press.

Booysen, H.A.S., & Eloff, J.H.P., (1995), A Methodology for the development of secure Application Systems. In proceeding of the 11th IFIP TC11 international conference on information security, IFIP/SEC'95.

Chokhani, S., (1992), Trusted products evaluation. Communications of the ACM. Vol. 35, Issue 7, pp. 64-76.

Chua, W.F., (1986), Radical Developments in Accounting Thought. Accounting Review, vol. 61, issue 5, pp. 583-598.

Code of Practice for Information Security Management, (1993), Department of Trade and Industry. DISC PD003. British Standard Institution, London, UK.

Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and General Model. May 1998, Version 2.0, CCIB-98-026.

Cooper, J.A., (1989), Computer and Communications Security: Strategies for the 1990s. McGraw-Hill, New York, USA.

Custance, N.D.E., (1996), The use of baseline measures in risk assessment. Proceedings of the 30th Annual International Carnahan Conference on Security Technology. IEEE Computer Society Press.

Dhillon, G., (1997), Managing Information Systems Security. MacMillan Press LTD, UK.

Dhillon, G. & Backhouse, J., (2000), Information system security management in the new millennium. Communications of the ACM, Volume 43, Issue 7, pp. 125-128.

Dhillon, G. and Backhouse, J., (2001), Current directions in IS security research: toward socio-organizational perspectives. *Information Systems Journal.* Vol 11, No 2.

Evans, A.S. & Welling, A.J., (1999), UML and the formal development of safety-critical real-time systems. IEE Colloquim on Applicable Modelling, Verification and Analysis Techniques for Real-Time Systems.

Ferraiolo, K., & Sachs, J.E., (1996), Distinguishing Security Engineering Process Areas by Maturity Levels. Proceedings of the 9th Annual Canadian Information Technology Security Symposium.

Finne, T., (1995), The Information Security Chain in a Company. Computers & Security. Vol. 15, No. 4, pp. 297-316.

Fisher, R.P., (1984), Information Systems Security. Prentice-Hall, New Jersey, USA.

Fites, P. & Kratz, M.P.J., (1993), Information Systems Security: A Practitioner's Reference. Van Nostrand Reinhold, New York, USA.

Fitzgerald, K.J., (1995), Information security baselines. Information Management & Computer Security, Vol. 3 Issue 2, pp. 8-12.

Fitzgerald, K.J., (1993), Risk Analysis: Ten Years On. Information Management & Computer Security, Vol. 1, issue 5.

Freeman, J.W. & Neely, R.B., (1993), On security policy modeling. Proceedings of the eight Annual Conference on Computer Assurance (COMPASS'93).

Freeman, J.W., Darr, T.C., Neely, R.B. (1997), Risk Assessment for large heterogeneous systems. proceedings of the 13th Annual Computer Security Applications Conference.

Galliers, R.D., & Land, F.F., (1987), Choosing appropriate information systems research methodologies. Communication of the ACM, vol. 30, no. 11, pp. 900-902.

Galliers, R.D., & Swan, J.A., (1997), Against structured approaches: information requirements analysis as a socially mediated process. Proceedings of the Thirtieth Hawaii International Conference on Systems Sciences, IEEE Society Press.

Garfinkel S. & Spafford G., (1997), Web Security & Commerce. O'Reilly & Associates, Inc. USA.

Garvey, T.D., (1992), The Inference Problem for Computer Security. Proceedings of the Fifth Computer Security Foundations Workshop. IEEE Computer Society Press.

GASSP, (1999), Generally Accepted System Security Principles (GASSP). Version 2.0. Information Systems Security. June, vol. 8, no. 3

Gollman, D., (1999), Computer Security. Wiley & sons, UK.

Guarro, S.B., (1987), Principles and Procedures of the LRAM Approach to Information Systems Risk Analysis and Management. Computer & Security. Issue 6, pp. 493-504.

Halliday, S. Badenhorst, K., von Solms, R., (1996), A business approach to effective information technology risk analysis and management. Information Management & Computer Security, Vol. 4 Issue 1, pp. 19-31.

Hefner, R., (1997b), A process standard for systems security engineering: development experiences and pilot results. Third IEEE International 1997 Software Engineering Standards Symposium and Forum, Emerging International Standards (ISESS 97).

Hirschheim, R., (1985), Information systems epistemology: An historical perspective. In: Research methods in information systems. E. Mumford et al. (eds), Elsevier Science Publisher.

Hirschheim, R., Klein, H. K., & Lyytinen, K., (1995), Information Systems Development and Data Modelling: Conceptual and Philosophical Foundations. Cambridge University Press, UK.

Iivari, J. & Kerola, P., (1983), A Sociocybernetic framework for the feature analysis of information systems design methodologies. In T.W. Olle, H.G. Sol, C.J. Tully (eds.), Information Systems Design Methodologies: A Feature Analysis. Pp. 87-139, North-Holland, Amsterdam.

Iivari, J & Koskela, E., (1987), The PIOCO model for IS design, MIS Quarterly, Vol. 11, No. 3, pp. 401-419.

Iivari, J., (1989), Levels of abstraction as a Conceptual Framework for an Information Systems. In E. D. Falkenberg and P. Lindgreen (eds): Information System Concepts: An In-depth Analysis. North-Holland, Amsterdam.

Iivari, J. and Hirschheim, R., (1996), Analyzing information systems development: A comparison and analysis of eight IS development approaches, Information Systems

Information Technology Security Evaluation Criteria (ITSEC) (1990), Harmonised Criteria of France, Germany, The Netherlands and the United Kingdom.

IT Baseline Protection Manual, (1996), BSI, Germany.

Jackson, F., (1980), Ontological Commitment and Paraphrase. Philosophy, Vol. 55, no. 213, pp. 303-315.

James, H.L., (1996), Managing information systems security: a soft approach. Proceedings of the Information Systems Conference of New Zealand. IEEE Society Press.

Järvinen, P., (1997), The new classification of research approaches. The IFIP Pink Summary - 36 years of IFIP. Edited by H. Zemanek, Laxenburg, IFIP.

Jung, C., Han, I., & Suh, B., (1999), Risk Analysis for Electronic Commerce Using Case-Based Reasoning. International Journal of Intelligent systems in Accounting, Finance & Management. Vol. 8, issue 1, pp. 61-73.

Kahn, J.J., & Abrams, M.D., (1994), Editorial: why bad things happen to good systems, and what to do about it. Proceedings of the 10th Annual Computer Security Application Conference. IEEE Computer Society Press.

Klein, H., & Lyytinen, K., (1985), The Poverty of Scientism in Information Systems. pp. 131-161. In: Research methods in information systems. E. Mumford et al. (eds), Elsevier Science Publisher.

Klein, H.K., Myers, M.D., (1999), A set of Principles for Conducting and Evaluating Interpretative Field Studies in Information Systems. MIS Quarterly, Vo. 23, No. 1, pp. 67-94.

Lichtenstein, S., (1996), Factors in the selection of a risk assessment method. Information Management & Computer Security, Vol. 4 Issue 4, pp. 20-25.

Lyytinen, K., (1987), A Taxonomic Perspective of Information Systems Development: Theoretical Constructs and Recommendations. In R. Boland & R. A. Hirschheim (eds): Critical Issues in Information Systems Research, John Wiley & Sons, Ltd., pp. 3-41.

Mathiassen & Munk-Madsen, A., (1986), Formalizations in System Development. Behaviour and Information Technology, Vol. 5, No. 2.

Mautner, T., (1996), A Dictionary of Philosophy. Blackwell Publishers Ltd, Oxford, UK.

Mingers, J.C., (1995), Information and Meaning: foundations for an intersubjective account. Information Systems Journal, Vol. 5, no. 4, October, Pp. 285-306.

Moore, GE., (1903), Principia Ethicia, Cambridge, UK.

Moses, R., (1995), Corporate risk analysis and management strategies. Proceedings of the European Convention on Security and Detection. IEEE Computer Society Press.

Moulton, R. T., & Moulton, M. E., (1996), Electronic Communications Risk Management: A Checklist for Business Managers. Computer & Security, Vol. 15, No.5.

Murine, G.E. & Carpenter, C. L., (1984), Measuring Computer System Security Using Software Security Metrics. In Computer Security: A global challenge, J.H. Finch and E.G. Dougall (eds.). Elsevier Science Publisher.

Nitzberg, S.D., (1999), The Cyber Battlefield: Is This The Setting for the Ultimate World War? Proceedings of Military Communications Conference (MILCOM). Vol. 1. IEEE Computer Society Press.

Niiniluoto, I. ,( 1999),Critical Scientific Realism. Clarendon Library of Logic and Philosophy, Oxford University Press, Oxford, UK.

Norman, A.R.D., (1983), Computer Insecurity. Chapman & Hall, NY, USA.

Nunamaker, J.F., Chen, M., Purdin, T.D.M., (1991), Systems development in information systems research. Journal of Management Information Systems, vol. 7., no. 3., pp. 89-106.

Ockham, W., (1990), Philosophical Writings: A selection. Hackett Publishing Company, Indianapolis, USA.

OECD, (1996), Guidelines for the Security of Information Systems. OECD, Paris, France.

O'Leary, T.J., Goul, M., Moffitt, K.E. & Radwan, A.E., (1990), Validating expert systems. IEEE Expert, Vol. 5, Issue 3, pp. 51-58.

Overbeek, P.L., (1995), Common Criteria for IT Security Evaluation - Update Report. Proceedings of the IFIP TC11 Eleventh International Conference on Information Security, IFIP/SEC'95.

Ozier, W., (1999), Risk Analysis and Risk Assessment. Handbook of Information Security Management (eds): M. Krause and H.F. Tipton, CRC Press LLC, Florida.

Pap, A., (1949), Elements of Analytic Philosophy.

Parker, D. B., (1998), Fighting Computer Crime - A New Framework for Protecting Information. Wiley Computer Publishing. USA.

Parnas, D.L. Schouwen, J. & Kwan, S.P., (1990), Evaluation of Safety-Critical Software. Communications of the ACM, Vol. 33, No. 6, June, pp. 636-648.

Payne, C.N., Froscher, J.N., McDermott, J.P., (1990), On models for a trusted application system. Proceedings of the Sixth Annual Computer Security Applications Conference.

Schaefer, M., (1989), Symbol security condition considered harmful. Proceedings of 1989 IEEE Symposium on Security and Privacy.

Seager, M. Guaspari, D., Stillerman, M & Marceau, C., (1995), Formal Methods in THETA kernel. Proceedings of the 1995 IEEE Symposium on Security and Privacy.

Sherwood, J., (1996), SALSA: A Method for Developing Enterprise Security Architecture and Strategy. Computers & Security. Vol. 15, no. 6, pp. 501-506.

Siponen, M.T., (2001a), An analysis of the recent IS security development approaches: descriptive and prescriptive implications. In: G. Dhillon (eds:) Information Security Management - Global Challenges in the Next Millennium, Idea Group (2001).

Siponen, M.T. (2001b): On the scientific background of information security management standards: a critique and an agenda for further development. The Second Annual Systems Security Engineering Conference), 28 February – 2 March, Orlando, Florida, USA.

Solms, R., (1997), Can Security Baseline replace Risk Analysis? Proceedings of the IFIP TC11 13th International Conference on Information Security (SEC'97), 14-16 May, Copenhagen, Denmark.

Solms, R., (1998), Information security management (3): the Code of Practice for Information Security Management (BS 7799). Information Management & Computer Security. Vol. 6, Issue 5, pp. 224-225.

Solms, R., (1999), Information security management: why standards are important. Information Management and Computer Security, Vol. 7, Issue 1, pp. 50-58.

Spruit, M. & Samwel, P.H., (1999), Risk analysis on Internet connection. Proceedings of the IFIP TC11 WG11.2/WG11.2 Seventh Annual Working Conference on Information Management & Small Systems Security.

SSE-CMM, (1998a), The Model. v2.0. http://www.sse-cmm.org.

SSE-CMM, (1998b), The Appraisal Method. v2.0. http://www.sse-cmm.org.

Stacey, T.R., (1996), Information Security Program Maturity Grid. Information Systems Security. Vol. 5, No.2.

Thomas, R.K. & Sandhu. R.S. (1994). Conceptual Foundations for a Model of Task-based Authorizations. Proceedings of the 7th IEEE Computer Security Foundations Workshop.

Walsham, G., (1996), The Emergence of Interpretivism in IS research. Information Systems Research, Vol. 6, No. 4, pp. 376-394.

Veatch, J.D., James, J.W., Bosma, P.H., May, T.T., Garner, D.W., Priem, R.G., (1995), Requirements Driven Methodology for conducting risk analyses on unclassified networks. Proceedings of the 29th Annual International Carnahan Conference on Security Technology.

Williams, J.G. & Abrams, M.D., (1995), Formal methods and models. In: Information Security - An integrated Collection of Essays. Edited by M. D. Abrams, S. Jajodia & H. J. Podell. IEEE Computer Society Press, Los Alamitos, California, USA.

Winograd, T. & Flores, F., (1986), Understanding Computers and Cognition. Addison Wesley Publishing Company, USA.

Wong, K.K., (1977), Risk analysis and control: a guide for DP managers. NCC Publications, Southampton, UK.

Wood, C.C., Banks, W.W., Guarro, S.B., Garcia, A.A., Hampel, V.E., Sartorio, H.P., (1987), Computer Security: A Comprehensive controls Checklist. John Wiley & Sons.

Zhou, D., Kuo, J.C., Older, S., Chin, S. K., (1999), Formal development of secure email. Proceeding of the 32nd AnnuaI Hawaii International Conference on Systems Sciences.