Advent of ISO/IEC 27001 Certification and its Role In Initial Inter-organizational Trust

Nikolas Prezas

Candidate for M.Sc. In Analysis Design and Management of Information Systems
Information Systems and Innovation Group
Department of Management
London School of Economics

In the competitive global village we live in, organizations have realized that information security has become a critical business function. Companies are no longer able to fully protect their own information technology (IT) environments, since they have little control over the IT systems with which they link. Building upon over ten years of development, the information security industry has agreed upon and published the international standard ISO/IEC 27001 for Information Security Management Systems. This study provides a review of this international standard and, utilizing a trust model as a theoretical lens, goes on to examine the role of this standard in facilitating initial interorganisational trust. Conclusions are then drawn, including a recommendation that further rigorous examination is required in the form of empirical studies.

1. Introduction

> *" The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards – and even then I have my doubts "*
>
> **Eugene H. Spafford**[1]

Nowadays organizations increasingly rely on information technology (IT), which makes IT security a very important field for guaranteeing business continuity (Von Solms & Von Solms, 2005). The majority of companies interlink their IT systems as a result of connecting to electronic data interchange (Reekers & Smithson, 1996) and the Internet. This interconnection holds an information security risk for an organization (Solms, 1999). Companies attempt to protect their own IT environment, but unfortunately they have little control over the IT systems with which they link. In the case that those external IT environments are not secure, it may create a threat to their own IT systems (Straub & Welke, 1998). Accordingly, certification of one's IT security approach assures collaborating companies a certain level of reliability and trust (Fenz, Goluch, Ekelhart, & Weippl, 2007; Wilson, 1997).

According to the Department of Trade and Industry (DTI), the annual cost of information security breaches in the UK was estimated for 2006 to be £10 billion pounds (Information Security Breaches Survey, 2006). Moreover, 2004 survey findings by DTI revealed that 74% of the overall respondents suffered a security incident during the previous year (as opposed to 44% in 2002, and 24% in 2000). Such incidents (Schneier, 1998; Willison & Backhouse, 1998) can result in financial loss, damage to the organization's reputation, disruption in business continuity, and legal liabilities. The head of security and privacy services at Deloitte UK recently stated that the protection of organizations' data has never been under such intense scrutiny, that now this is expected to be a board level issue, and that ignorance is no longer an excuse. [2]

With these facts in mind, organizations would do well to ensure that they are appropriately protected. One of the fundamental approaches to achieving this is to follow international standards. According to "Information Security Breaches 2006" by PriceWaterhouseCoopers, corporations certify their Information Security Management System (ISMS) according to international standards in order to increase their equity. ISO/IEC 27001, which is the first in the ISO/IEC standards family, is one such certification standard.

The next section presents a review of the literature regarding the ISO/IEC 27001 certification. This is followed by a brief explanation of the trust model proposed by McKnight (1998). The trust model is then used as a theoretical lens in order to examine the role of the standard in the production of initial inter-organizational trust.

2. Literature Review

2.1 Defining ISO/IEC 27001 Certification

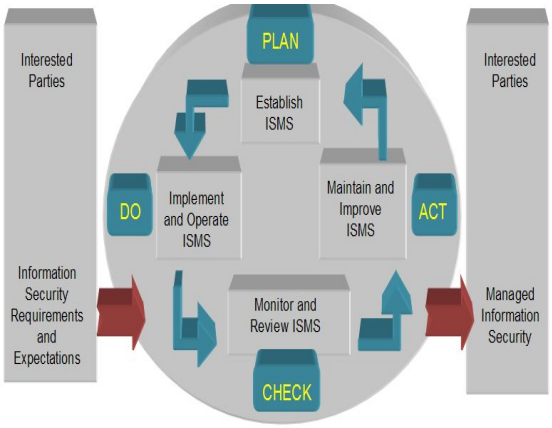
The term "certification" describes a process whereby a product or a process is tested and evaluated to determine whether or not it complies with a specific standard (Eloff & Solms, 2000). A "standard" includes unified regulations and simplified necessary timely conditions that provide a way of measuring objects, procedures, duties, concepts of power and so on, based on fair, just and convenient opinions (Fung, Farn, & Lin, 2003). These unified regulations and conditions need an "authority" to see that all parties adhere to these regulations (Solms, 1999). For that reason, written guarantees of compliance are issued by certification authorities (CAs) verifying that products, procedures, and services of a company comply with the procedures or activities specified in the regulations (Fung, Farn, & Lin, 2003).

Furthermore, a substantial goal of a demanding standard is to become an international, authoritative and generic standard (Siponen, 2005). Thus one of the value measures of a standard is to become incorporated by the International Organisation for Standardization (ISO), an association based in Switzerland which establishes international certification standards in several fields.[3] In October 2005, ISO and the International Electrotechnical Commission (IEC)[4], after establishing a joint technical committee, ISO/IEC JTC 1, and building upon over ten years of development (Backhouse, Hsu, & Silva, 2006), formed the specialized system for worldwide standardization. As a result organizations can now be certified under the new ISO/IEC 27001 international standard (ISO/IEC 27001:2005). Some organizations will be certified for the first time, with others converting from existing BS7799 certifications (Mann & Richardson, 2006).

ISO/IEC 27001:2005 is an evolution on British Standard BS7799, which addresses the definition of requirements for information security management systems (Mann & Allison, 2006). According to ISO/IEC 27001:2005:

> *"This International Standard has been prepared to provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System (ISMS)".*

The "Plan-Do-Check-Act" (PDCA) model is adopted in this international standard in order to structure all ISMS processes. The next figure outlines the PDCA model and demonstrates how an ISMS utilizes the information security requirements and expectations of the stakeholders as input to produce accurate, functioning, and effective information security results (ISO/IEC 27001:2005).



PDCA model applied to ISMS processes (adopted from ISO/IEC 27001:2005)

The ISO/IEC 27001 process approach first highlights the significance of understanding an organization's information security requirements and the need for information security policies and objectives (Plan). Second, it points out how implementing and operating controls are important in managing information security risks, specifically within the context of the corresponding business risks (Do). Third, it emphasizes the need to monitor and review the performance and effectiveness of a company's ISMS (Check). Finally, it highlights the importance of continuous improvement based on objective measurement (Act) (ISO/IEC 27001:2005).

According to BS 7799 (the predecessor of the international information security standard) as well as ISO/IEC 27001, the three elements of information security – confidentiality, integrity and availability – are completely upheld by the standard. In essence, the first element requires that only authorized users can access the information. The second one requires that information is kept accurate through proper safeguarding and the third one requires that information and associated assets are accessible to the appropriate people when needed (BS 7799:1995; ISO/IEC 27001:2005;). Moreover, Thomas Peltier, a certified information systems security professional (CISSP) and president of a security consulting company, indicates that confidentiality, integrity and availability need to be the pillars of an effective information security management within an organization (Peltier, 2003).

The following table outlines the controls of the new ISO/IEC 27001 as published by ISO on October of 2005.

Controls of ISO/IEC 27001
1. Security policy
2. Organization of information security
3. Asset management
4. Human resources security
5. Physical and environmental security
6. Communications and operations management
7. Access control
8. Information systems acquisition, development and maintenance
9. Information security incident management *
10. Business continuity management
11. Compliance

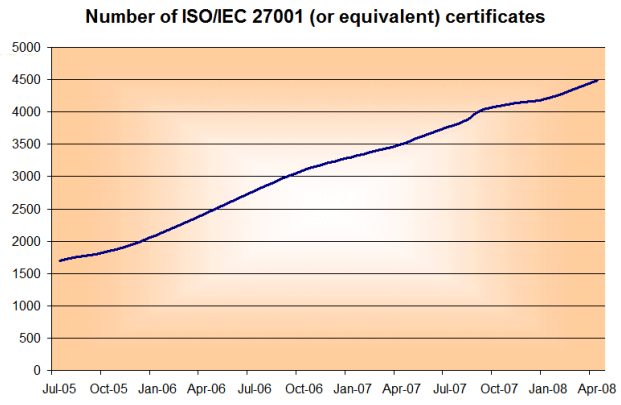
This control was added after the adoption of BS 7799 Part 2 by ISO in 2005.

Ted Humphreys, who was a convenor of the group for the development of the ISO standard stated[5]:

> *" The publication of ISO/IEC 27001:2005 is a big event in the world of information security and the standard has been eagerly awaited. It is a standard that all security-conscious organizations should look to implement."*

2.2 Widespread adoption of ISO/IEC 27001

Many certification bodies become accredited by national standards bodies, such as the British Standards Institution and the National Institute of Science and Technology, in order to be able to issue certificates by reviewing compliance with the international standard ISO/IEC 27001. More than 4,400 organizations all over the world have already been certified with ISO/IEC 27001 or equivalent certifications[6]. The following graph[7] shows the total number of ISO/IEC 27001 certifications over the last two and a half years.



What is remarkable is that although companies are not required to be certified by the standard, an increasingly demand by organizations of different types is noticeable by observing the data above. The reason is that the adoption of ISO/IEC 27001 within organizations results in a number of benefits above and beyond simple compliance, which all together lead to ensuring business continuity (Freeman, 2007).

2.3 ISO/IEC 27001 Ensures Business Continuity

Numerous authors support that the advent and subsequent adoption of ISO/IEC 27001 definitely ensures business continuity (Fenz, Goluch, Ekelhart, & Weippl, 2007; Freeman, 2007; Mann & Richardson, 2006). According to JTC1/SC27[8], the ISO/IEC 27001 standard has several different features that ensure business continuity including:

- ensuring that security risks are cost effectively managed;
- ensuring compliance with laws and regulations;
- ensuring that the specific security objectives of an organization are met;
- determination of the status of information security management activities by the management of organizations;
- determination of the degree of compliance with the policies, directives and standards adopted by an organization by the internal and external auditors;
- provision of relevant information about information security policies, directives, standards and procedures to trading partners and other organizations with whom they interact for operational or commercial reasons; and
- provision of relevant information about information security to customers.

The next section focuses on the benefit which is engendered by the last two types of use. That benefit is the production of the initial interorganisational trust which is conducive to business continuity.

3. ISO/IEC 27001 and Initial Interorganisational Trust

3.1 Defining Initial Interorganisational Trust

According to Pavlou (2002), interorganisational trust can be defined as "the subjective belief with which organizational members collectively assess that a population of organizations will perform potential transactions according to their confident expectations, irrespective of their ability to fully monitor them".

Initial trust refers to trust in an unfamiliar trustee, a relationship in which the actors do not yet have credible, meaningful information about, or affective bonds with, each other (Wingreen & Baglione, 2005).

As stated earlier, organizations have little control over the IT systems with which they link due to the increased connectivity created by EDI and the Internet (Solms, 1999). Thus, trust becomes an infrastructure requirement, like a firm's operating system or its network (Wilson, 1997), in a world where trust is difficult to establish due to the impersonal environment (Pavlou, 2002).

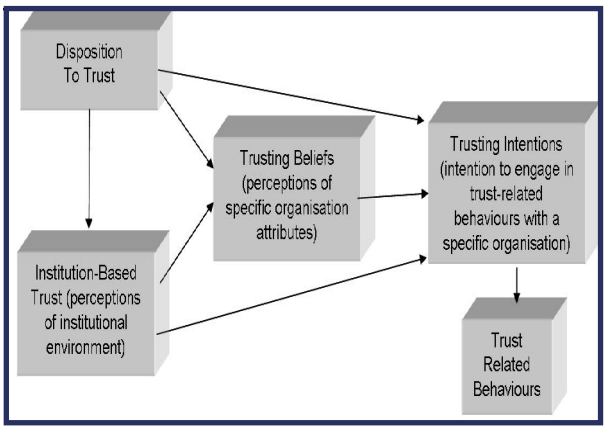
According to ISO/IEC 27001 (first edition), the standard is "designed to ensure the selection of adequate and proportionate security controls that protect information assets and give confidence to interested parties". Therefore one of the main aims of ISO/IEC 27001 is the production of confidence and subsequently of trust among the organizations.

However, according to Pavlou (2002), in order to achieve the production of interorganisational trust, institutional trust is first needed due to the fact that the latter acts as proxy for the former. It is stated that institutional trust is the most essential approach by which trust is produced in an impersonal economic environment. Institutional trust can be described as "the belief that a party has about the security of a situation because of guarantees, safety nets and other structures" (Shapiro, 1987). Two types of institutional trust mechanisms are third party certification and escrows (Zucker, 1986 cited within Pavlou, 2002). ISO/IEC certification is an example of the first type. Thus, the adoption of this standard within organizations may contribute to a large extent in the production of interorganisational trust and especially of initial trust among organizations (before parties have meaningful information about each other).

3.2 Initial Trust Model

It was decided to use the McKnight trust model as a theoretical lens because it includes institution-based trust as well as the more common trust types—trusting intentions, trusting beliefs, and disposition to trust. This model was also chosen because the aim is to examine the influence of ISO/IEC 27001 to interorganisational trust before the organizations have meaningful information about each other. Thus this "Model of Initial Formation of Trust" was considered to be the most appropriate for the purposes of this study.

The constructs of the McKnight trust model are being integrated within the broad framework of the Theory of Reasoned Action (TRA) (Fishbein & Ajzen, 1975; McKnight, Choudhury, & Kacmar 2002). TRA posits that beliefs lead to attitudes, which lead to behavioural intentions, which lead to the behaviour itself. Applying TRA to the trust model, it is then posited that trusting beliefs (perceptions of specific organization attributes) lead to trusting intentions (intention to engage in trust-related behaviours with a specific organization), which in turn result in trust-related behaviours. The figure below shows the model of initial trust formation integrated within the framework of the TRA.



Model of Initial Trust Formation integrated within the framework of the TRA (McKnight, Choudhury, & Kacmar, 2002)

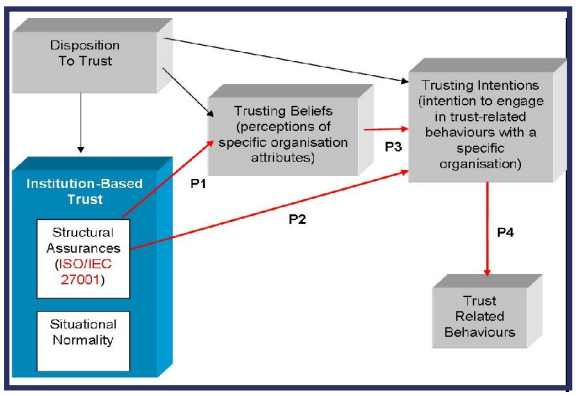
Furthermore, institution-based trust and disposition to trust are posited as antecedents to trusting beliefs and intentions. Institution-based trust is the sociological dimension of trust (McKnight, Choudhury, & Kacmar, 2002). It refers to an organization's perceptions of the institutional environment – in

this case, the international standard. Perceptions of the structural characteristics of the international standard, such as security and international recognition, can influence trusting beliefs and trusting intentions toward a specific organization. Disposition to trust means a general propensity to trust others, which can also influence an organization's beliefs and intentions towards a potential collaborating organization. However our attention in this study will be on the first antecedent, the institution-based trust, and not on disposition to trust.

In the following section, the constructs of the proposed model are analysed and discussed, in order to examine the influence of the international standard ISO/IEC 27001 to the initial interorganisational trust.

3.3 Analysis and Discussion

The following is a depiction of the trust model as it modified by the author in order to show the significance of ISO/IEC 27001 as an element of institution-based trust.



ISO/IEC 27001 as a part of structural assurances to examine its influence in the proposed model

3.3.1 Trust-Related Behaviours

It is posited that interorganisational trust is gained only after each party has both engaged in trust-related behaviours and assessed the "trustworthiness" of the collaborating organization by observing the consequences of those behaviours. In this case, we use the above trust model to examine only the first aspect, the engagement in trust-related behaviours. This is because the aim is to examine how and to what extent the internationally established standard ISO/IEC 27001 influences an organization's engagement in trust-related behaviours with a potential collaborating company. We examine only the standard's influence on the initial interorganisational trust and not on the ongoing trust relationship.

Trust-related behaviours are actions that demonstrate dependence on a collaborating organization, that make the trusting organization vulnerable to the collaborating one, or increase its risk. For instance, such behaviours in inter-organizational coordination are sharing confidential information or entering into a transaction.

3.3.2Institution-Based Trust

Institution-based trust (Bjorck, 2004) is the belief that necessary structural conditions are present to enhance the probability of achieving a successful outcome in an endeavour like the interconnection of organizations. McKnight (1998) describes two dimensions of institutional trust – structural assurances and situational normality. Structural assurances are "beliefs that favourable outcomes are likely because of contextual structures, such as contracts, regulations, and guarantees". Situational normality refers to "beliefs that success is anticipated because the situation is normal". In this case, we take the International standard ISO/IEC 27001 as an element of structural assurances in order to examine its influence in the proposed model.

Establishing ISO/IEC 27001 within organizations, structural assurance belief is likely to affect trusting beliefs for several reasons. First, believing that a situation is bounded by principles enables an organization to believe that the participants in the situation are trustworthy. This international standard provides a robust information security management framework for implementing the principles of OECD Guidelines (2002)[9], governing the security of information systems and networks. These OECD principles, which are reflected by the PDCA model, govern risk assessment, security design and implementation, security management, reassessment, response, awareness, and responsibility (ISO/IEC 27001:2005).

Moreover with this standard, structural assurance belief will stay consistent with all the produced trusting beliefs. That is due to the fact that this standard advocates checking on a routine basis that the existing controls are working effectively. As the UK Audit Commission reports for 1994, 1998, and 2001 showed, many firms fail to check whether their controls are operating as intended (Willison & Backhouse, 1998). As a result, those safeguards which are failing to perform leave an information system vulnerable. The ISO 27001, however, upholds compliance reviews at managerial and technical levels[10]. Apart from the compliance reviews, which are a part of the Check phase, the standard also advises organizations to address new and emerging risks to their systems. The standard emphasizes that organizations can identify their security requirements by using risk assessment techniques. By doing that, companies can identify their risks and implement the requisite controls, which is a part of the Act phase. This characteristic of the standard is extremely important for the production of trusting beliefs because as Willison & Backhouse (1998) stated, just as organizations change in terms of business practices and resources, so do the security functions, and with change come new risks.

Thus, the following proposition is suggested:

> *Proposition 1: In the initial attempt of an interorganisational coordination, the adoption of the international standard as a part of the institution-based trust will tend to produce high levels of trusting beliefs.*

The fact that ISO/IEC 27001 is the only internationally recognized standard for an information security management system and that now all the trading partners conform to the same standard enables organizations to feel assured about their expectations of the other party's future behaviour. The perception that the two world's largest developers of international standards, ISO and IEC, collaborated for the development of a mutually accepted standard will probably lead to the direct effect on trusting intentions. As a consequent, the following proposition is made:

> *Proposition 2: In the initial attempt of an interorganisational coordination, the per-*

ception that the ISO/IEC 27001 is the only internationally recognized standard for information security management systems will tend to directly lead to trusting intentions.

3.3.3Trusting Beliefs: Perceptions of Specific Organisation Attributes

Trusting beliefs refers to the confident truster perception that the trustee, a specific potential collaborating organization, has attributes that are beneficial to the truster. As mentioned at the beginning, ISO/IEC 27001 reinforces the three attributes of information security – confidentiality, integrity, and availability. Thus the international standard provides fundamental attributes that can be beneficial to the truster. Furthermore, the management of risk, which is provided by the standard, is a process that includes the prevention, detection, and response to incidents, ongoing maintenance, review, and audit. All of these aspects, which are encompassed in the Plan, Do, Check and Act phases, are conducive to the three aforementioned attributes. As a result, if an organization believes that the other party has confidentiality, integrity, and availability as the pillars of its information security, then it is likely to form a trusting intention toward that party. Therefore, the third proposition that is suggested is the following:

Proposition 3: In the initial attempt of an interorganisational coordination, trusting intention will be a function of confidentiality, integrity, and availability which are totally upheld by the international standard ISO/IEC 27001.

3.3.4Trusting Intentions: Intention to Engage in Trust-Related Behaviours

Trusting intentions refers to the truster being securely willing to depend, or intends to depend, on the trustee (McKnight, 1998). The standard's developers stated that "implementation of ISO/IEC 27001 will reassure customers and suppliers that information security is taken seriously within the organizations they deal with because they have in place state-of-the-art processes to deal with information security threats and issues"[11]. Considering this and the previous discussions, we can suggest that in the initial attempt of an interorganisational coordination, trusting intentions originated either from the trusting beliefs (confidentiality, integrity, and availability) or directly from the institution-based trust (due to the standard's international recognition) will produce a high probability of engagement in trust-related behaviours. Therefore we finally have the beginning of the production of initial interorganisational trust. Therefore, the last proposition is the following:

Proposition 4: In the initial attempt of an interorganisational coordination, trusting intentions originated from the adoption of ISO/IEC 27001 as a part of institution-based trust, will produce a high probability of engagement in trust-related behaviours and as a result lead to initial interorganisational trust.

Considering the propositions above, we see that the international standard positively influences the production of initial interorganisational trust to a high level. However, it may not apply in the same way to the maintenance of interorganisational trust. For ongoing trust between organizations, the adoption of this international standard may not influence in a major way the sustainability of interorganisational trust (although the positive influence is obvious) and many other factors are more important, such as escrows, testing, and back and forth operations. Like any relationship, trust is built over time, starting with shared understandings (standards in this case) but actually built and grown with mutually acceptable practices in the long run.

4. Conclusion

This study presented the international standard ISO/IEC 27001 followed by an investigation of its role in initial interorganisational trust. It is clearly seen that the adoption of this standard within organizations positively influences the production of intercompany trust. Although the sustainability of trust among firms certified by this international standard has not been examined in this study, the use of the initial trust model by McKnight (1998) as a theoretical lens clearly shows that the establishment of this standard produces a high probability of the production of initial interorganisational trust.

However, future empirical validation is definitely needed to validate the propositions revealed by this study and show that international standard ISO/IEC 27001, as a part of institutional trust, could engender initial interorganisational trust. Moreover, it would be interesting to empirically assess the relative effect of the standard to the ongoing interorganisational trust by examining how and to what extent this international standard affects the consequences of trust-related behaviours and the subsequent sustainability of intercompany relationships.

In general, given the impersonal nature of the electronic environment and the extensive use of IT, organizations now recognize that information is their greatest asset and that information security is a critical business function. The ISO/IEC 27001 standard has emerged as the recognized mechanism to improve the security of information exchange, and more importantly, to make judgements about others. Organisations are now being asked about ISO/IEC 27001, particularly by national and local government entities and financial sector customers. This is being driven by adoption of the standard as part of their legal and regulatory compliance. Others are seeing a competitive advantage in leading their sector and using certification in information security management to develop customer confidence and win new business (Mann & Richardson, 2006). With more public concern over security issues, there is now a requirement to build effective mechanisms in order for the organizations to demonstrate that they can be trusted.

References

Backhouse, J., Hsu, C. W., & Silva, L. (2006). Circuits of Power in Creating de jure Standards: Shaping the International IS Security Standard. *MIS Quarterly, 30*(Aug 06 Sup), 413-438.

Bjorck, F. (2004). Institutional theory: a new perspective for research into IS/IT security in organizations. *Proceedings of the 37th Annual Hawaii International Confer-*

ence on System Sciences.

BS 7799:1995. Code of practice for Information security management. *British Standards Institute*.

Eloff, M. M., & Solms, S. H. (2000). Information Security Management: A Hierarchical Framework for Various Approaches. *Computers & Security, 19*(3), 243-256.

Fenz, S., Goluch, G., Ekelhart, A., & Weippl, E. (2007). Information Security Fortification by Ontological Mapping of the ISO/IEC 27001 Standard. *In 13th Pacific Rim International Symposium on Dependable Computing, PRDC2007. IEEE Computer Society*.

Fishbein, M., & Ajzen, I. (1975). Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research. *Addison-Wesley, Reading, MA*.

Freeman, E. H. (2007). Holistic Information Security: ISO 27001 and Due Care. *Information systems security, 16* (5), 291-294.

Fung, A. R.-W., Farn, K.-J., & Lin, A. C. (2003). A Study on the Certification of the Information Security Management Systems. *Computer Standards and Interfaces, 25* (5), 447-461.

Information Security Breaches Survey. (2006). *PriceWaterhouseCoopers*,http://www.pwc.co.uk/pdf/pwc_dti-fullsurveyresults06.pdf

ISO/IEC 27001:2005.—Information Technology – Security Techniques – Information Security Management Systems – Requirements. *Published by ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commision)*, Available at ANSI [http://www.ansi.org/].

Mann, I., & Allison, L. (2006). From BS 7799 to ISO 27001. *ECSC*, Information Security Risk Management.

Mann, I., & Richardson, H. (2006). ISO 27001 Executive Brief. *ECSC*, Information Security Risk Management.

McKnight, D. H. (1998). Initial Trust Formation in New Organizational Relationships. *The Academy of Management review, 23*(3), 473-490.

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and Validating Trust Measures for e-Commerce: An Integrative Typology. *Information Systems Research, 13*(3), 334-359.

Pavlou, P. A. (2002). Institution-Based Trust in Interorganizational Exchange Relationships: The Role of Online B2B Marketplaces on Trust Formation. *Journal of Strategic Information Systems, 11*(3-4), 215-243.

Peltier, T. R. (2003). Preparing for ISO 17799. *Information systems security, 11*(6), 21-28.

Reekers, N., & Smithson, S. (1996). The role of EDI in inter-organizational coordination in the European automotive industry. *European Journal of Information Systems, 5* (2), 120-130.

Schneier, B. (1998). Security Pitfalls in Cryptographic Design. *Information Management and Computer Security, 6*(3), 133-137.

Shapiro, S. P. (1987). The Social Control of Impersonal Trust. *The American journal of sociology, 93*(3), 623-658.

Siponen, M. (2005). An Analysis of the Traditional IS Security Approaches: Implications for Research and Practice. *European Journal of Information Systems, 14*(3), 303-315.

Solms, R. V. (1999). Information Security Management: Why Standards are Important. *Information Management and Computer Security, 7*(1), 50-57.

Straub, D., & Welke, R. (1998). Coping With Systems Risks: Securing Planning Models for Management Decision Making. *MIS Quarterly, 22*(4), 441-469.

Von Solms, B., & Von Solms, R. (2005). From Information Security to… Business Security? *Computers & Security, 24*(4), 271-273.

Willison, R., & Backhouse, J. (1998). Opportunities for Computer Crime: Considering Systems Risk from a Criminological Perspective. *European Journal of Information Systems, 15*(4), 403-414.

Wilson, S. (1997). Certificates and Trust in Electronic Commerce. *Information Management and Computer Security, 5*(5), 175-181.

Wingreen, S. C., & Baglione, S. C. (2005). Untagling the Antecedents and Covariates of E-Commerce Trust: Institutional Trust vs. Knowledge-Based Trust. *Electronic Markets, 15*(3), 246-260.

Footnotes

[1]Professor of Computer Science, Purdue University

[2]Comment by Mike Maddison, UK head of security and privacy services at Deloitte, on 19 March of 2008 (http://www.deloitte.com/dtt/press_releases).

[3]ISO is the world's largest developer of International Standards. It was established in 1947 in Geneva, Switzerland. Although ISO's principal activity is the development of technical standards, ISO standards also have important economic and social repercussions (http://www.iso.org/iso/about.htm).

[4]The IEC was founded in 1906 and is the world's leading organization that prepares and publishes international standards for all electrical, electronic and related technologies (http://www.iec.ch).

[5]http://www.ansi.org.

[6]http://www.iso27001certificates.com (visited May 5, 2008).

[7]http://www.iso27001security.com/html/27001.html (visited May 5, 2008).

[8]The ISO/IEC committee responsible for the ISO/IEC 27001 standard (http://www.din.de/ni/sc27/).

[9]OECD (Organisation for Economic Co-operation and Development) Guidelines for the Security of Information Systems and Networks – Towards a Culture of Security. Paris: OECD, July 2002. www.oecd.org.

[10]This supported by the last (11th) control area, Compliance, which is divided into the following controls: first, "compliance with legal requirements"; second, "compliance with security policies and standards and technical compliance"; and third, "information systems audit considerations".

[11]http://www.ansi.org.

About the author

Nikolas Prezas, graduated from the National Technical University of Athens, with a five-year BSc & MSc degree in Applied Mathematics and Physical Sciences. He carried out a six-month project on ERP Systems, before coming to the London School of Economics to pursue the Analysis, Design and Management of Information Systems masters programme. His specialisation is on Information Risk & Security and his dissertation research focuses on the implementation and adoption of ISO/IEC 27001 within the context of Cyprus.