**IASME: Information Security Management evolution for SMEs,**

Richard Henson, Worcester Business School,
Daniel Dresner, Head of Information Assurance NCC,
David Booth, Independent Security Consultant

## 1. Abstract

Most of the research in information risk and risk management has focused on the needs of larger organisations. In the area of standards accreditation, the ISO/IEC 27001 Information Risk Management standard has continued to grow in acceptance and popularity with such organisations, although not to a significant extent with SMEs. An interesting product recently developed for ENISA (European Nations Information Security Association) based on the Carnegie-Mellon maturity model and aimed at SMEs has not so far filled the gap.

In this paper, a researcher and two practitioners from the UK discuss an innovative development in the UK for addressing the information assurance needs of smaller organisations. They also share their perceptions about the security of national information infrastructures, and concerns that SMEs do not get the priority that their position in the supply chain would suggest they should have.

The authors also explore the development and roll out of IASME (Information Assurance for SMEs), which they have developed in the context of a tight market, where spare cash is in short supply, and many SMEs are still in survival mode. The question for the business is therefore not seen as "can we afford to spend on information security" but "can we afford not to spend…" As well as the effect on being able to do business at all of having an SMEs systems compromised, there are also matters of reputation, and the growing threat of fines as a result of not complying with laws and regulations.

The paper concludes with achievements of real businesses using the IASME process to cost-effectively achieve information assurance levels appropriate for themselves.

SME, Information Risk Management, Information Security Management Systems, Data Protection Legislation, Value of Data, ISO/IEC 27001, PCI DSS. ISMS

## 2. Introduction

IASME came about as a result of a successful bid to the UK Technology Strategy Board for funding on an Information Infrastructure Protection project (Technology Strategy Board, 2009). The makeup of the consortium is believed to have contributed to the success of the bid, in that it provided research facilities (University of Worcester), development expertise (David Booth) and business structure (National Computing Centre). This is reflected in the contributions to this paper. The focus of the project has initially been SMEs in the West Midlands of the UK, and supporting them in the setting up management systems for their information security (ISMS). Previous research (Coles-Kemp & Overill, 2007) had previously shown that the setting up of an ISMS was considered to be problematic for many SMEs.

The information security of SMEs is important not just because the business itself could have its vital information compromised and infringe Data Protection legislation (EU, 1981; HMG, 1998) and/or go out of business, but also because of the links that SME will have to other businesses across the supply chain. An alert to supply chain vulnerability, and its potential for exploitation by CyberTerrorists, was first identified after the 9/11 attack (Sheffi, 2001), and recent research has shown that up to 1/3 of security incidents are caused by vulnerabilities in links with external partners. It is therefore not just in the interest of a given SME to have an effective ISMS, but also in the interest of every other business that has dealings with that SME.

In spite of this, surveys consistently show the low priority of information security and its management (or assurance) within SMEs. The authors of this report were dismayed that high profile UK security breaches that caused great embarrassment to the organisations concerned (Nationwide, 2007; HMG, 2007) had little impact on SMEs. It was suspected that the 2007-8 recession and the need to demonstrate ROI for any expenditure were responsible (Henson & Hallas, 2008), but there was no evidence of any change in SME behaviour in this respect as the effects of the recession began to subside (Arthur, 2009).

## 3. The Development of IASME

The IASME consortium was already aware of the lack of research available on the reasons why SMEs were reluctant to develop ISMSs, and to expand of this body of knowledge was part of the brief for the project. Findings relating to SMEs are summarised in the IASME Research document (IASME, 2010). Research updates continued throughout the funded part of the project, and the scrutiny of private sector surveys on aspects of information security continues to present day. Consequently, and in the light of new experience, the IASME process and standard are continually under review.

The R & D phase of the project had the following stages:

1. Relevant research on information security in SMEs
2. Development work based on principles of ISO/IEC 27001 and research findings
3. Piloting the developed IASME model with typical SMEs
4. Modification and re-piloting of the IASME model to produce a service and product that can be used to help SMEs to cost-effectively create their own ISMSs.

The next stage (current) is the development of a business model, and launching and marketing of IASME as a commercial product with associated services to support SMEs wishing to have robust information security. At the time of writing, the product has been launched, and a business model has been devised. Marketing and promotion will follow.

### 3.1 Research Phase

This was unlike conventional academic research, because the majority of available research on information security has been conducted by governments and in the public sector. The apparent lack of academic interest in information security has been reported elsewhere (Fomin & deVries, 2008). The multidisciplinary field known as "Economics of Information Security" has flourished in recent years, although it only received greater prominence in the UK from 2007, when a massive security leak in a government department hit the headlines (HMG, 2007). The annual WEIS conference was held in the UK in 2009, but none of the papers accepted focused on security needs of SMEs. This provoked one of the authors to analyse contributions to this esteemed conference over the previous seven years (Appendix 1), This revealed no papers with SME or SMB in the title out of a total of 160 papers delivered. It may be that some of these papers involved SMEs in their content, and this informal exercise was just intended to highlight the lack of research.

Thankfully, there have been a number of academic contributors to the debate in recent years, and some useful research on information security management habits of SMEs has been undertaken. However, SME is a broad term, and no research appeared to have been done that looked at differences between the three groups identified by the EU, classifying by no. of employees (EU, 2005). There are SMEs all over the world, and there are different classifications of size. At a previous Atiner SMEs conference, there was a certain amount of disagreement about what constituted an SME, and indeed in North America the normal terminology is SMBs (small and medium sized businesses) with maximum sizes of 100, and 500 respectively (Marketing Playbook, 2009). This paper will focus on the EU definition, and, to differentiate, will refer as appropriate, to SME10 (1-10 employees) SME50 (11-50 employees) and SME250 (51-250 employees).

Some seminal academic research on SME information security actually took place in Southern Africa, before BS7799 became an International Standard. Here, a model was proposed (von Solms, 2001) for an incremental approach to BS7799, acknowledging the difficulty, but worthiness, of the then BSI standard. An MBA thesis relating to the difficulties involved in making BS7799 more approachable for SMEs resulted in a significant academic paper, which appeared just prior to the International Standard (Upfold & Sewry, 2005), and influenced subsequent UN recommendations (United Nations, 2005). SME research continues in Africa. In Europe the best and most recent SME-focused research that the consortium could find from within the EU have been another paper from Barlette (Barlette & Fomin, 2008), a study of German SMEs conducted in 2007/8 (Kluge & Sambasivam, 2008), and more recently a study in Spain (Sanchez et al, 2009). These all provided useful input for developing the IASME model, as did Pacific studies involving a maturity model and SMEs based in Taiwan (Chiang et al, 2008), and a study relating to SME culture in Australia (Dojkovski et al, 2007). Five years after Coles-Kemp's SME focus groups, the University of Worcester carried out its own research (Arthur, 2009), and this revealed further insights into not only the low level of priority attributed to information security, but also some of the reasons why many of them apparently had such little apparent interest in engaging with information security.

UK Government-backed research (BERR, 2008) provides information security related data including SMEs on an annual basis. This was used extensively to provide longitudinal analysis, and because it was felt that this would carry considerable weight as we sought suitable SMEs to participate as IASME pilots. Another useful source was the EU-backed body ENISA, and in particular the work of Poettinger (2008), which resulted in a "quick-and-easy" risk assessment tool for SMEs.

There was, and continues to be, a rich vein of private sector research. In particular, the consortium found that the detailed studies provided by Verizon (Verizon, 2009a, 2009b) Symantec (Symantec 2010) and PGP Corporation (PGP, 2010), where there was differentiation within the data that fitted SME organisational sizes. Much of the best private sector research tends to refer to US SMB definitions of smaller businesses, but again the annual basis of the surveys was very useful for showing trends.

These reports were also produced on an annual basis, which, in conjunction with the BERR reports, were very useful for monitoring trends. They have confirmed the suspicions highlighted by IASME and others that as larger businesses threw greater resources at protecting their networks, the previously unnoticed small businesses would be perceived as "weak links". The IASME consortium had previously suggested that this would not only compromise the security of the SMEs themselves, but also would potentially provide back doors into the networks of larger organisations who are supply chain partners. The information security of SMEs should therefore be of considerable interest to their larger supply chain partners. It was interesting that the University of Worcester's 2010 survey confirmed the trend identified in the annual security breach reports for larger companies to require some sort of evidence of an SME developing an ISMS before they agree to share data with them. This trend is still in its early stages, but does seem to be accelerating.

### 3.2 Creation of the draft IASME standard

As regards the development of an information security standard for SMEs, surprisingly little activity has been found from any country. In a previous paper for an Atiner SME conference (Henson & Hallas, 2009), the lack of support for small businesses in existing security standards, including ISO/IEC 27001 had been highlighted. The metamorphosis of BS7799 (BSI, 1999) into ISO27001 (ISO, 2005) had been welcomed by Coles-Kemp & Overill in their 2007 paper, but these authors felt that this was still not addressing the problem as far as smaller businesses were concerned. Certainly a risk assessment that would cross-reference with 134 security controls can be readily seen to be quite a daunting task that needs considerable human and financial resources.

Earlier research comparing standards had been summarised by Kluge & Sambasivam, 2008, and had confirmed the authors' perception that, ISO/IEC 27001 was the most comprehensive. It therefore made sense that this should form the basis of any information assurance standard for SMEs. One of the consortium members, David Booth, already had extensive experience in this area, and is a member of the SC27 committee that is involved with the production and continual development of the ISO/IEC 27001 standard (ISO, 2011) and is familiar with other sources of information security guidance. He had been working for some time to develop something that

would be readily accessible to SMEs. This would clearly take time, and plenty of user feedback. It was decided that the best approach would be an iterative development with actual SMEs working in different sectors of industry.

### 3.3 Research on existing software tools that can be used with SMEs

Information risk assessment had been shown by the earlier University of Worcester research (Arthur, 2009) to be particularly inaccessible as far as West Midlands SMEs were concerned. It was hoped, even anticipated, that tools would be available that would assist with the information risk assessment process. However, the tools that were reviewed tended to be more suited to larger organisations, with top-down management structures and clearly defined processes. One reviewed tool had been developed by Joachim Poettinger (Poettinger, 2009) and was adopted by ENISA (European Network and Information Security Agency) and this proved to be sufficiently easy to use with SMEs to provide useful information about the nine main areas of information risk, for a particular organisation. For more comprehensive risk assessment that would be able to highlight specific controls, a more rigorous tool would be needed, but for a quick analysis, and to get the SME on board with information risk assessment, this was an effective tool to use.

Earlier studies reported by Coles-Kemp and Overill in their 2007 paper, had suggested that SMEs were only interested in the security of "high risk" processes. This would clearly be a concern to be addressed in the development of the new standard and process, and a risk assessment model would need to be developed that would be able to take into account a process of assessing risk for all information and information flows, without becoming too cumbersome for the business. Whilst this was considerably challenging, the potential goal seemed so worthwhile that it was agreed that the consortium would seek to either find such a tool or (if it proved that existing tools were not scalable and/or suitable), develop their own or adapt an existing model.

## 4. Development of the IASME standard

Most small businesses have grown up around a core business concept, and prefer not to become distracted by (perceived) peripheral activities. It is necessary to present information assurance (IA) as part of core business, providing essential support, in the same way as auditing, accounts, inventory, payroll and similar functions. These latter functions are thought of as traditional parts of any business, while IA is relatively new, but just as important.

The importance of these functions will vary from organisation to organisation, but all will apply to some extent. The IASME process reduces the complexity inherent in this list using a structured method suitable for SMEs.

Business Security Functions:

**Organisation:** manage information resources within the organisation and in the organisation's relations with partners.
**Risk:** understand and manage the risk to your business information.
**Policy:** establish management direction and communications.

**Assets:** know your information assets, and acquire and dispose of them securely.
**People:** know your people and educate them in business security.
**Things:** protect your information assets from physical harm.
**Malware:** defend your information from hostile attack and be ready to recover from infection.
**Access:** control who and what can access your information.
**Planning:** build security and privacy in at the start; make sure you have the right-sized information systems.
**Operations:** manage and monitor your information systems effectively.
**Mistake Management:** ensure breaches of confidentiality, integrity or availability of your systems are detected and dealt with; learn the lessons !
**Continuity:** make sure you can recover quickly from partial or total loss of key information assets.
**Legal Compliance:** know what is required and make sure you comply.

### 4.1 Initial draft

It was important that the consortium produce an initial draft as quickly as possible based on experience and research input, which could be used with SMEs to get the development of the IASME process underway. This initial development was entirely the work of David Booth, based on his knowledge of ISO/IEC 27001, and other sources of guidance. ENISA, SANS and COBIT also provided useful input on control selection. The total number of security controls was only slightly smaller than ISO/IEC 27001, but only a limited number were identified as essential, and the application of the others would depend on the target risk profile, so for a particular SME the number of controls they would need to consider would likely to be lower than for a full implementation of ISO/IEC 27001.

This first draft of the IASME standard was tidied up and clarified for use with SMEs in the spring of 2010. The standard uses a Risk Profile to indicate one of three identical control sets, where each has the same Essential controls, but the remainder of the controls are prioritised according to the risk profile (i.e. Not Applicable, Desirable, Highly Desirable). These priorities can be varied by the Assessor for an individual Target of Evaluation (ToE) if necessary as a result of the Risk Profiling process. It was important that this rather novel approach was well tested and refined during the development stage.

### 4.2 First iteration, based on SME input

Although the IASME Consortium and the University of Worcester had previously been in contact with SMEs, it was felt that representative pilots should be sought, and these were selected at random, in terms of those who responded to a questionnaire on Information Security that had been circulated. The questionnaire, which was also intended for research purposes, is included here as Appendix 2. There were unfortunately not a sufficient number of responses for a statistically significant analysis of responses, but the exercise served its other purpose in providing some SMEs to become pilot organisations for the IASME process. Each pilot would get free consultation, guidance, and all documentation in the initial development year.

Initial contact was face-to-face, and generally took between one and two hours. One long-established principle of ISO/IEC 27001 is that information security has to be the responsibility of senior management. However, this principle is often found lacking in the information management of SMEs that have not seriously thought about developing an ISMS. For this reason, whenever possible, the CEO of the organisation was directly involved. This was not always possible, especially with larger SMEs. However, because a number of questions involved senior management and their decision-making, no progress could be made without the latter's input. This happened via proxy if necessary, but the completion of required information took longer in such cases.

Although the IASME process is intended for all SMEs, part of the initial assessment process is to establish the size and complexity (in terms of sensitivity of data and connections with external partners) of the organisation; generally the larger and more complex, the higher the potential risk. The combination was used to classify each organisation as "low", "medium" or "high" risk. Depending on the classification, more stringent controls would be expected to obtain IASME Gold for a high risk organisation, in terms of IASME classification.

**4.3 Revisions of the IASME Documentation and Guidance**

A number of significant minor revisions occurred as the pilot SMEs engaged with the process, to minimize the burden of administration in order to gather evidence that processes were in place, and evidence of compliance with requirements of the standard. The version of the IASME standard v1.0a included as appendix 3 with this paper is the latest version.

Much was learned during the pilot phase about what worked and what didn't, both from the viewpoint of the study team and the businesses. One of the assumptions was that time and money could be saved both by standardising the process and involving the business. This included developing and supplying templates of key documents in a non-technical form intelligible to the business, including a policy structure, an outline management structure and a business continuity template. In addition, the risk profiling was adapted from ENISA and other guidance to present the primary risk arenas in an environment which would be understood by, and self-completed by the business (with the oversight of the Assessor).

It turned out that the structure of the policy document could incorporate key management commitments, thereby providing the basis of an information security management system. Further, by incorporating commitment to the essential controls, it could provide the basis of a fast-track improvement and assessment process, particularly suitable for micro-businesses of less than 10 people, as long as their risk profile remained Simple. Businesses whose risk profile falls outside these parameters will continue to be assessed using the normal processes.

The original concepts were shown to work effectively in practice with some minor modifications. Of the three businesses assessed during the pilot stage, one succeeded using the fast-track process the remainder were assessed using the normal processes. Involvement of the business had the useful by-product of providing some basic information security management education, a factor which the businesses found useful. Case studies of three pilot businesses can be found on the IASME web site.

One of the principles behind developing IASME was to make a complex process involving risk assessments of many processes and decision-making about many security controls as easy as possible for the business. This meant that as much information as possible was provided within the documentation, and all that was needed for the business to do was confirm the elements of their normal practice, and supply evidence. Even so, a number of pilots dropped out of the process due to lack of time, as the documentation evolved to the more streamlined v1.0, which was unfortunate. It was accepted that SMEs would often need more "hand holding" with administration than had originally been anticipated, and an expectation that they would find the time to read through guidance documents and provide written or digital materials without more direct intervention. A provision for extra face-to-face time was built into the funding model for IASME, which is outlined in section 7.

## 5. The Assessment and Grading Process

The assessment process consists of a Risk Profile Assessment, followed by either a Fast Track and/or a Full Matrix Assessment. The RPA has developed from an initial manual, rather subjective assessment to a balanced scorecard method, in which answers to a questionnaire are weighted and summed to provide a fully documented and repeatable result. The FTA is also a balanced scorecard questionnaire, while the FMA is currently a spreadsheet calculation. These methods are subject to continual improvement; one target is to make much of the documentation and calculation available on-line.

Both the FTA and FMA paths result in a graded assessment: Improvement Required, Bronze, Silver or Gold. Three levels of achievement are considered to offer a way for under-achieving businesses to improve at their own pace, and this proved to be effective during the pilot stage. In the latter three cases, a certificate is awarded to the business and their certification is published on the IASME web site. In all cases the Assessor will provide an improvement plan, which the business can follow if they wish to move up to a higher grading. After the first assessment, businesses are re-inspected at least once a year and a full re-assessment is carried out every three years (at present). The business must also inform IASME if there are any material changes to the risk profile between inspections. These inspections are necessary to retain the certificate, which will be withdrawn (and publicised) if these conditions are not met.

Examples of documentation provided for pilot participants and the latest version of the IASME standard is provided at Appendix 3.

## 6. Successful IASME Completions

To date, three of the dozen or so SMEs that became IASME pilots have seen the process through to certification, and one small company that had already achieved ISO/IEC 27001 has been through the assessment process and obtained IASME Gold certification. All received their certificates at the IASME launch, earlier this year (IASME, 2011a). The consortium is often asked which SME sector they are targeting with IASME, and the answer is, genuinely, that SMEs in all sectors can, and indeed should, benefit. The three successful completers to date are one retail company, one web design company, and one computer security company. One is a large SME, and the other two are microbusinesses. Their experiences with engagement with the IASME process are reported on the website (IASME, 2011b), and echo the

consortium members perception that this is a valuable product for SMEs, with much to offer in terms of offering protection against breaches, greater understanding of businesses processes involving information, and potential mitigation against action from the ICO (Information Commissioner's Office) under the 1998 Data Protection Act, in the event of a breach.

## 7. Production and Implementation of Business Plan

The pilots got everything free of charge, including their IASME certificates. Looking beyond the pilots, IASME will need to be self-funding. A funding model based on fixed costs plus extras based on size and complexity of the organisation was developed in association with colleagues at NCC (National Computing Centre), who also proposed a model for training and development of existing ISO/IEC 27001 or equivalent auditors who wish to become IASME assessors. As with another scheme developed by NCC for accreditation of good practice in IT departments, incentives will be offered to assessors who come across other SMEs wishing to improve their information security management.

Marketing will therefore expand IASME as a business through referrals. However, it is anticipated that only a small number of leads will be generated through referrals, and plans for direct marketing to SMEs are currently being developed. One option is to work in partnership with existing ISO/IEC 27001 auditing companies; they gain through taking the SME from IASME Gold standard to ISO/IEC 27001 standard, and IASME gains indirectly through referral of companies ultimately seeking ISO/IEC 27001 certification, but only in the early stages of ISMS development. Two such organisations have already expressed an interest in such a partnership.

## 8. Conclusion

A lot has been achieved already through the research & development effort with actual SMEs to create the IASME process and standard, and engaging with prospective partners in the ISO/IEC 27001 certification marketplace to serve common interests. The review of investigations from around the world was very useful in establishing why SMEs – particularly smaller SMEs - are fundamentally different from larger companies, have different information systems, and are less willing to engage with information security processes. Direct input from working with the pilots also revealed the human resources pressures on SMEs compared to larger organisations which usually have some spare resource that can be used to gather the information required for risk assessment, procedure and policy development, and other aspects of an information security mechanism. Moreover, because the SME often is already working at full human resource utilisation levels, there would be no-one spare to look after an information security management system even if the human resource had been found to set such a thing up.

In the UK, only small amounts of public money has been used to support the small business in developing a secure information infrastructure, with an apparent expectation that what happens on a large scale can be scalable to the SME. This filtered down into providing support for larger organisations as the law tightened up as a result of the data loss incidents of 2007, and anticipating that SMEs will find assistance through regional, professional, or industry bodies. IASME consortium

members would like to think that with their funding from the Technology Strategy Board, they have developed a service and information security standard that can be used at modest cost by any small business wishing to develop an ISMS, provide legal compliance, and protect their precious information assets.

## 9. References


Arthur J, (2009), "Information Security survey of SMEs for Worcester Business School".

Barlette Y & Fomin V V, (2008), "Exploring the suitability of IS security management standards for SMEs", paper presented at the 41st Hawaii International Conference on System Sciences, Hawaii.

BSI, (1999), "British Standard BS7799 part 2", British Standards Institute.

Chiang T J, Chang Ray-I, Kouh J S, Hsu K P, (2008), "An Information Security Education Maturity Model", 2008 International Conference on Computer & Network Technologies in Education (CNTE2008), pub: 25-31 Aug. 2008, pp.224-231.

Coles-Kemp E & Overill E R, (2007), "The Design of Information Security Management Systems for Small-to-Medium Size Enterprises".

Dojkovski, S, Lichtenstein, S and Warren, M, (2007), "Fostering information security culture in small and medium size enterprises: an interpretive study in Australia", in Proceedings of the 15th European Conference on Information Systems, University of St. Gallen, St. Gallen, Switzerland, pp. 1560-1571.

ESRC, (2008), "Press Releases, 2008, June: Wake-up call to business: Tighten up on Information Security", ESRC Society Today, June 2008.

EU, (2005), "SME definition: User guide and model declaration". Available at http://ec.europa.eu/enterprise/enterprise_policy/sme_definition/sme_user_guide.pdf

Hansard, (2007), "HM Revenue and Customs, The Chancellor of the Exchequer (Mr. Alistair Darling)", available [On-line] at http://www.publications.parliament.uk/pa/cm200708/cmhansrd/cm071120/debtext/71120-0004.htm

HMG, (1998), "Data Protection Act", Her Majesty's Stationary Office.

IASME, (2010), "Research Findings", available [On-Line] at http://iasme.ncc.co.uk/index.php?option=com_content&view=article&id=12

IASME, (2011b), "Certificate Holders", available [On-Line] at http://iasme.ncc.co.uk/index.php?option=com_content&view=article&id=11

IASME, (2011b), "Certificate Holders", available [On-Line] at http://iasme.ncc.co.uk/index.php?option=com_content&view=article&id=9

ISO, (2005), ISO/IEC 27001:2005, International Standards Organisation.

ISO, (2011), "JTC 1/SC 27: IT Security techniques", available [On-Line] at: http://www.iso.org/iso/iso_technical_committee.html?commid=45306

Kluge D, & Sambasivam S, 2008, "Formal Information Security Standards in German Medium Enterprises", The Proceedings of CONISAR 2008, 1533, pp.1-12. Available [on-line] at http://isedj.org/isecon/2008/1533/index.html

Marketing Playbook (2009), "SMB - Definition of B2B Marketing and Sales Terminology", http://www.marketing-playbook.com/glossary/index.php/term/%26%23160%3B,SMB.xhtml

PGP Corporation, (2010), "2009 Annual Study: UK Cost of a Data Breach".

Symantec, 2010, "Symantic 2010 SMB Data protection Survey".

Sánchez L E, Parra A S-O, Rosado D G, Piattini M, (2009), "Managing Security and its Maturity in Small and Medium-sized Enterprises", Journal of Universal Computer Science, vol. 15, no. 15 (2009), 3038-3058
Sheffi Y, (2001), "Supply Chain Management under the Threat of International Terrorism", International Journal of Logistics Management, Vol. 12 Issue 2, pp.1-11
Technology Strategy Board, 2009, "Information Infrastructure Protection: Managing complexity, risk and resilience. March 2009 Competition For Funding".
United Nations, (2005), "Regulations, Policies and Legal Frameworks Related to ICT: International Management Standards for ICT Development in the Greater Mekong Subregion" Part Four: Information Security: ISO17799:2000 for survival and Business Continuity.
Upfold C.T., & Sewry D.A., (2005), An Investigation Of Information Security In Small and Medium Enterprises (SMEs) in The Eastern Cape", Rhodes University.
Verizon, (2009a), "2009 Data Breach Investigations Report", Verizon Business.
Verizon, (2009b), "2009 Data Breach Investigations Supplementary Report: Anatomy of a Breach", Verizon Business.
von Solms B, (2001), "Incremental Information Security Certification", Computers & Security, Volume 20, Issue 4, 31 July 2001, Pages 308-310.