The current issue and full text archive of this journal is available at
www.emeraldinsight.com/1754-2731.htm

Improving the quality of information security management systems with ISO27000

Alan Gillies
Hope Street Centre, Liverpool, UK

Abstract

Purpose – The ISO27001 standard provides a model for "establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System (ISMS)". This paper seeks to consider the global adoption of the ISO27000 series of standards, and to compare them with the adoption rates for ISO9000 and ISO14000. The paper aims to compare the barriers to adoption for the different standards.

Design/methodology/approach – Previous studies suggest that ISO27001 adoption is slower than for the other standards. The uptake of ISO27001 has been slower than the related management system standards ISO9001 and ISO14001, with approximately half the certifications compared with ISO14001. In response to the issues raised in this analysis, the paper considers how an approach based on a maturity model can be used to help overcome these barriers, especially in smaller companies.

Findings – The 2008 survey of ISO27001-certificated companies found that 50 per cent of the certificated organisations which responded had fewer than 200 employees, and were therefore in the SME category. Perhaps more surprisingly, around half of these had fewer than 50 employees The framework has used the ISO27002 code of practice to define the elements, which should be considered within the ISMS. Each element is then developed through a maturity model lifecycle to develop processes to the point where an ISO27001-compliant ISMS can be implemented.

Originality/value – The principal contribution of the paper is a step-by-step framework designed to simplify the process for organisations working towards ISO27001 and offer significant benefits at milestones before systems are mature enough to achieve certification.

Keywords ISO 9000 series, ISO14000, ISO27001, Total quality management, Information security, Incremental approach

Paper type Research paper

1. Introduction

Information security is a major issue for businesses, public bodies, their clients and the public. A quick survey of the media show that the risks apply to public and private bodies, to paper and electronic information, from the failure to protect live data or the failure to dispose of archive information and can arise from deliberate actions or inaction.

In 2008 the UK Information Commissioner argues that the privacy of personal information has four dimensions of value:

(1) *Operational value*: viewed in this way, personal information is an asset for the organisation. As with any other asset, personal information needs to be protected to ensure it is used effectively within the organization, and that its operational effectiveness and efficiency is maintained. Protecting it in ways which protects people's privacy ensures that the additional asset value it has due to it being personal information is maintained.

The TQM Journal
Vol. 23 No. 4, 2011
pp. 367-376

1754-2731
DOI 10.1108/17542731111139455

(2) *Individual value*: viewed in this way, holding and using people's personal information introduces significant risks for the organisation. If it does not handle people's personal information with care, and does not respect people's privacy concerns and meet their expectations, the organisation can cause people distress or harm. In turn, this can rebound directly on the organisation, causing its reputation to be damaged. This risk is significant, and the organisation needs to manage it to protect itself from this risk, as well as to protect the individual.

(3) *Value to others*: there are others who may wish to use the information, whether for legitimate or improper purposes. This can arise if a legitimate purpose is undermined by the personal information not being handled in accordance with the data protection principles. It can also arise if another party, causes harm through fraud or distress through embarrassment to the people concerned. As with accidental disclosure leading to embarrassment or harm to an individual, damage can also be caused to the organisation itself, irrespective of whether they have influence or control over the third party using the information for nefarious purposes.

(4) *Societal value*: potential damage to reputation may be seen as a need to do the right thing. Society increasingly legislates to give the right to privacy a legislative basis such as the EU directive 95/46/EC7, (European Parliament, 1995) enshrined in UK law as the Data Protection Act (1998), and alternative legislation outside the EU, such as SOX8 and GLB9 in the US. From 1st April, the UK Information Commissioner has the right to impose fines of up to £500,000 for privacy breaches.

As with any valuable asset, companies need to manage the asset to protect it.

2. The ISO27001 standard

The ISO 27000 series of standards provide a standard against which an information security management system (ISMS) can be certificated. The origins of the ISO27001 (BS ISO, 2005a) and 27002 (BS ISO, 2005b) standards lie in earlier work by the UK DTI and BSI. The timeline is as follows:

1989 UK DTI publish a users' code of practice for information security.

1993 BS PD 003: A code of practice for information security management.

1995 BS7799-1: A code of practice evolved from BS PD003.

1998 BS7799-2: A certification standard for an information security management system.

1999 BS7799-1 and BS7799-2 aligned: the subsequent ISO17799 and ISO27002 standards are based on this version of BS7799-1.

2002 BS7799-2 is modified to incorporate the Plan-Do-Check-Act cycle, in order to align it with ISO9001. This version formed the basis for the subsequent ISO27001 release in 2005.

2005 ISO code of practice published for information security management as ISO17799 (June).

2005 ISO certification standard for an information security management system published as ISO27001 (October).

2007 ISO17799 renumbered to ISO27002: note that the 1 and 2 numbering is now reversed when compared with BS7799.

The ISO27001 standard provides a model for "establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System (ISMS)" (ISO, 2005a). As with ISO9001 and ISO14001, the standard is predicated on the assumption that if the process is correct, the outcome will be satisfactory. Early versions of ISO9001 in particular were criticized for emphasizing process over outcome and consistency over merit.

More recent implementations of all of these standards have therefore been built around the plan-do-check act cycle. Often attributed to Deming, who certainly made it famous, the cycle was pioneered by Shewhart (1939) at the Bell Laboratories in the US as part of his work on statistical process improvement. The relationship between ISO27001:2005 and ISO9001:2000 and ISO14001:2004 is shown in Figure 1.

3. Adoption of the ISO27001 standard

In 2007, Certification Europe surveyed firms that had been certificated against ISO27001 (Certification Europe, 2008). A total 312 responses were received from India, Ireland, Italy, Hong Kong, Japan, the UK, and the United States. This appears to be a sample of around 10 per cent of the firms certificated by the time of the study. The survey found that the IT Services and software development sector is the primary adopter of ISO 27001 worldwide, with just one quarter of all certifications in the survey. Of these, just over half (52 per cent) are classed as IT security consultants. Of certifications 14 per cent were public sector, typically IT departments of larger organisations.

The survey found that 50 per cent of the certificated organisations who responded, had under 200 employees, and therefore in the SME category. Perhaps more surprisingly, around half of these had less than 50 employees.

The survey found that 80 per cent of organisations sought certification to ISO 27001 as a means of gaining competitive advantage, with a lowly 28 per cent who had been required to gain certification as a condition of tendering for business, and in 16 per cent of cases certification had been a mandatory requirement of a customer.

The reality may be less clear cut, as competitive advantage may derive from the ability to address specific markets as from internal benefits, and many organizations may stop short of making certification mandatory but still expect suppliers to achieve certification.

A total 56 per cent of the organisations within the survey identified cultural change as the main challenge to be overcome. However, other barriers such as senior management support or a lack thereof (18 per cent in this survey) may well be more significant in a random sample or amongst companies without certification. A remarkably high 80 per cent of companies in this sample already had certification to ISO9001, and were likely to be both amenable and knowledgeable when implementing the ISO27001 standard.

Studies (Certification Europe, 2008; Fomin *et al.*, 2008); Davis *et al.*, 1993) all suggest that ISO27001 adoption is slower than for ISO9001 and ISO14001, with approximately

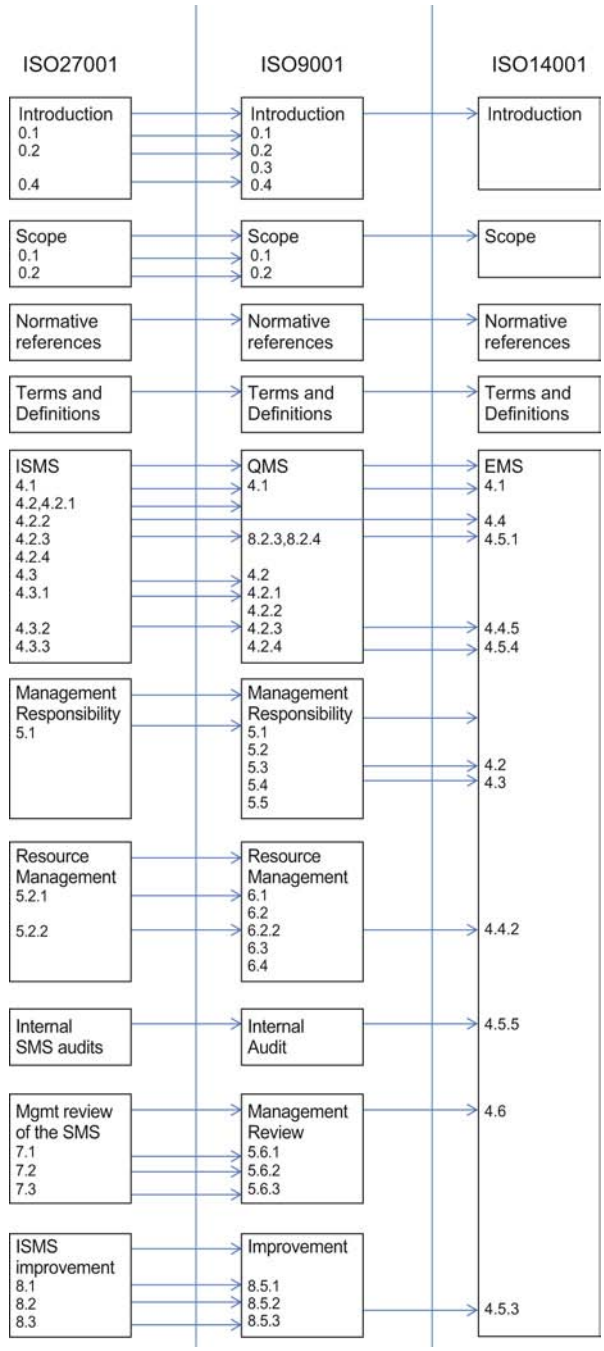

Figure 1.
Mapping of ISO27001 to ISO9001:2000 and ISO14001:2004

half the certifications when compared with ISO14001. It is also noticeable that the greatest uptake is by far is in Japan, where ISO27001 is mandated for many Government contracts. This slower uptake includes the majority of companies obtaining certification who already have previous ISO certification, and the effect of the Japanese Government mandating the standard.

4. Barriers to the adoption of the ISO27001 standard

Costs appear to vary but a common theme was the use of consultants with an average cost of £22,000. Whilst this figure is of limited value because of the wide range in size of the respondent companies, it does suggest that cost may be a barrier for many. Even amongst this group, 7 per cent stated that they would not use consultants, or alternatively reduce their reliance upon external resources if they were to implement the system again. It is suggested that poor consultancy support does not result in the transfer or establishment of a knowledge base within the client organisation. When the certification process is complete, the knowledge gained with the consultant and staff within the organisation lack ownership or understanding of the new system.

Fomin *et al.* (2008) use the longer experience of ISO9001 and ISO14001 certification to consider the barriers to adoption of ISO27001. They argue that the benefits of ISO 9001 certification have gradually shifted from earlier times when its certification was used as a signal to markets (Rodríguez-Escobar *et al.*, 2006) to one where firms can actually gain direct benefits from the effective use of the quality management system itself.

Backhouse *et al.* (2006, pp. 425-427) suggest that whilst this may be true in some cases for ISO/IEC27001, in the countries with the largest number of certificates for ISO/IEC 27001 the certification process is driven by either government regulation, as in Japan or supplier/buyer demands or the necessity of outsourcing and offshoring in markets such as Taiwan, Singapore and India.

Saint-Germain (2005) argues that an important driver for ISMS certification is demonstrating to partners that the company has identified and measured their security risks and implemented a security policy and controls that will mitigate these risks In addition, international invitations to tender are beginning to require that organizations be compliant with certain security standards, and security audit demands from financial institutions and insurance companies are increasing. A further incentive is lower insurance premiums for ISO 27001 certified companies (von Solms and von Solms, 2005).

5. Five stages to information security (5S2IS)

In order to reduce barriers to effective information security management, the author has developed a five step process (5S2IS) to encourage SMEs to implement systems even if they are not going to develop systems mature enough to be certificated against IS027001, which will protect the company against a range of risks to a level deemed adequate by the company.

5S2IS is built on the foundations of ISO27001, ISO27002 and the Capability Maturity Model (Humphrey, 1989).

The CMM is attractive, when compared to ISO standards because it allows for improvement and evolution. It can also be used in conjunction with other quality standards. The approach can highlight defects as they occur and this can both improve quality and feed information into internal ISO assessment, highlighting potential

non-conformances. The CMM prioritises tasks for improvement and provides a matrix of strengths and weaknesses. Paulk (1995) places ISO9000 practices between levels 2 and 3 in the CMM but argues that they are not directly comparable. The CMM and the ISO 9000 series of standards share a common concern with quality and process management. The two are driven by similar concerns and intuitively correlated. For this reason, the 5S2IS approach seeks to combine the best of both approaches. Schematically, the approach maps the plan-do-check-at cycle onto a five-stage development process, shown in Figure 2.

This translates into a two-dimensional information security matrix, with each dimension defined by a cell of the matrix at each of five development stages, shown in Figure 3.

For each cell of the matrix, the model defines:

(1) *Audit item*. This is the question, which defines the item to be audited within the ISMS.

(2) *Risk from inaction*. This explains the consequences of not taking action. This can be very important in gaining buy-in from staff, who may otherwise see the action as unnecessary.

(3) *Control*. This is the action required to address the audit item. If this measure is put in place, the item will be satisfied.

(4) *Measure*. This is the evidence, which may be used to demonstrate compliance with the audit item.

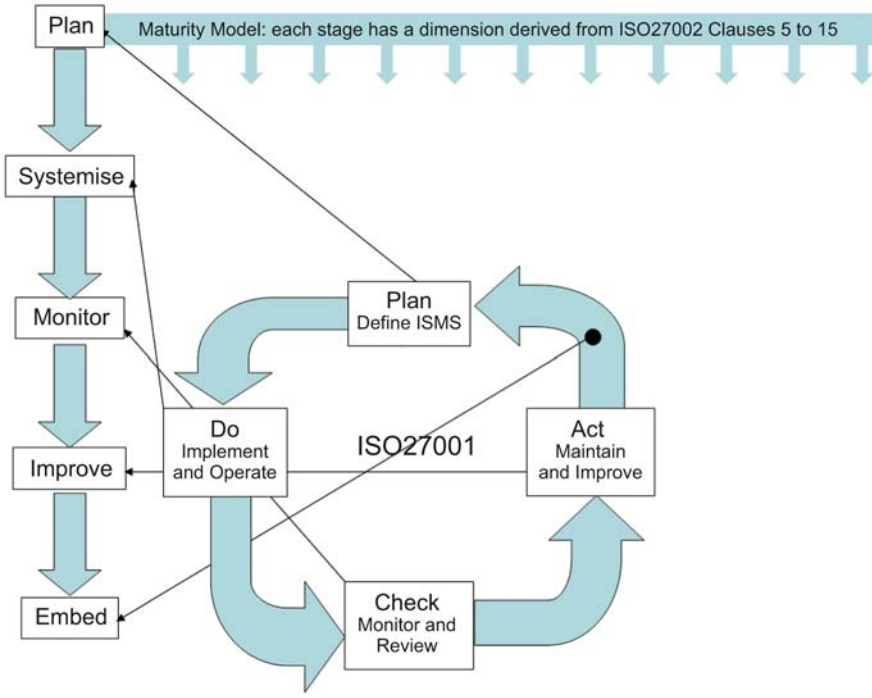

Figure 2.
Schematic diagram of incremental approach

	Security Policy	Organizing Information Security	Asset Management	Human Resources Security	Physical and Environmental Security	Communications and Operations Management	Access Control	Information Systems Acquisition	Development and Maintenance	Information Security Incident Management	Business Continuity Management	Compliance
1: Commitment												
2: Systematic												
3: Monitored												
4: Improving												
5: Embedded												

Figure 3.
Two-dimensional matrix to define incremental process

The author's previous experience with a similar model to embed innovation within similar companies (Howard and Gillies, 2009; Howard, 2010) has shown that such a step-by-step approach can overcome barriers to implementation by:

(1) Providing business benefits from a system which is at a lower state of maturity than is required by ISO27001.

(2) Motivating staff by successful achievement of milestones and demonstrable improvements with associated lowering of risks.

(3) Allowing a system to be implemented at a level appropriate to a small organisation.

(4) Embedding the model within a computer based tool to provide an efficient method of implementing the approach. The 5S2IS model can be provided within a PHP/SQL web database application.

6. Outline of the 5S2IS

The vertical dimension of the matrix is defined by the plan-do-check-act at the heart of ISO27001. If all five stages are completed for all dimensions, then the organization will have developed the capability to implement the complete cycle required for ISO27001 certification. At the start of the process, the original CMM defined processes as chaotic. This word is unduly dramatic for many organizations within the information security domain. A more apposite term might be sporadic or unsystematic. Many organisations have addressed information security issues in a piecemeal fashion, for example, imposing passwords, but not defining minimum standards for password strength or frequency of change. They may also have purchased software applications to address specific threats as viruses or Trojans, and put in place firewalls, but not educated staff about the ways they may inadvertently be breaching the firewall or placing information at risk of disclosure. The key to the 5S2IS approach is to draw together these disparate elements to systematise the approach. Each stage of the process reduces risk and further protects the information against risks:

(1) *Stage 1*. Draw up a plan. This stage is about defining smart goals for each of the dimensions to make explicit what the organization is seeking to achieve within

each information security dimension. As well as defining the goals, you will need to gain management sign up to the goals, to the process to be followed to reach these goals, and to the target stage to be reached and whether the ultimate goal is to demonstrate compliance with ISO27001 through external certification.

(2) *Stage 2*. Define a protocol for each of the smart goals defined in Stage 1. The protocol should define what the organization will do in order to achieve each goal. It will define the processes, and also outline compliance measures that will put in place to demonstrate whether the organisation is following the protocols themselves.

(3) *Stage 3*. Measure the organization's performance against the protocols from Stage 2. In particular, identify non-compliances with the protocols. This stage represents the implementation of the defined protocols. It will require the collection of monitoring data as defined in stage 2. It is also associated with significant cultural change within the organization as the protocols move from strategic commitment and then definition into implementation. It requires significant acceptance and ownership from staff across the organisation.

(4) *Stage 4*. Use the monitoring data from Stage 3 to improve performance and reduce non-compliances. This stage will require root cause analysis to identify underlying problems rather than superficial symptoms. By this stage, the organization has the ability to become a learning organization with regard to information security can achieve major improvements and gain significant business benefits

(5) *Stage 5*. Embed the improvement cycle within the organization. At this stage, the organization should have an ISMS compatible with ISO27001, and they may choose to move forward to ISO27001 certification, for verification, credibility and marketing purposes.

The horizontal dimension of the matrix is determined by the advice given in the code of ISO27002 code of practice. This gives rise to 11 dimensions:

(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 with legal and regulatory frameworks

Each dimension has activity defined at each stage of our five stage incremental process: it is important to complete all activities associated with a specific stage before moving on to the next one.

7. Conclusions

The problem of information security is becoming increasingly important for small and medium sized enterprises. In spite of this, the ISO27000 series of standards has only been slowly adopted. Evidence for the barriers to adoption suggests that the approach is overly complex and costly for many small organisations.

The author has developed an approach, known as 5S2IS, which builds upon the best of existing approaches but provides a stepwise approach which can be facilitated and mediated by technology to allow SMEs to protect their information without making a huge step change and investment which may not be appear to be commensurate with the risks.

5S2IS uses the ISO standards and the CMM to develop a two dimensional information security management matrix. This matrix can be used to implement a stepwise approach to information security management and can be encompassed within a computer-based tool to further reduce the barriers to adoption by small companies.

References

Backhouse, J., Hsu, C.W. and Silva, L. (2006), "Circuits of power in creating *de jure* standards: shaping an international information systems security standard", *MIS Quarterly*, Vol. 30, (special issue: Standard making: a critical research frontier for information systems research), pp. 413-38.

BS ISO (2005a), "BS ISO 27001 Information technology – security techniques – information security management systems – requirements", British Standards Institute, London, ISBN 0 580 46781 3.

BS ISO (2005b), "BS ISO 27002 Information technology – security techniques – code of practice for information security management", British Standards Institute, London, ISBN 978 0 580 59729 9 (Identifier of standard renumbered from (BS) ISO/IEC 17799 to (BS) ISO/IEC 27002, July 2007).

Certification Europe (2008), *ISO 27001 Global Survey: The Facts and the Figures Underlying the Growth of ISO 27001 World-wide*, Certification Europe, Dublin.

Data Protection Act (1998), *Chapter 29*, The Stationery Office, London.

Davis, C., Gillies, A.C., Smith, P. and Thompson, J.B. (1993), "Current quality assurance practice amongst software developers in the UK", *Software Quality Journal*, Vol. 2 No. 3, pp. 145-61.

European Parliament (1995), "On the protection of individuals with regard to the processing of personal data and on the free movement of such data", *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995, Official Journal L 281*, 23 November, pp. 0031-50.

Fomin, V.V., Kaunas, L., de Vries, H.J.Y. and Barlette, Y. (2008), "ISO/IEC 27001 information systems security management standard: exploring the reasons for low adoption", paper presented at the 3rd European Conference on Management of Technology, Industry-University Collaborations in Techno Parks, Nice, France, September 2008.

Howard, J. (2010), "Competent to innovate: an approach to personal development to improve innovation competency in SMEs", *Proceedings of the 5th European Conference on Entrepreneurship & Innovation, Athens, Greece*, in press.

Howard, J. and Gillies, A.C. (2009), "Knowledge to innovate: developing a tool to assess and assist the development of the capacity to innovate in small and medium-sized enterprises",

Proceedings of the 4th European Conference on Entrepreneurship & Innovation, Antwerp, Belgium, pp. 206-14.

Humphrey, W.S. (1989), *Managing the Software Process*, Addison-Wesley, Reading, MA.

Paulk, M.C. (1995), "How ISO 9001 compares with the CMM", *IEEE Software*, Vol. 12 No. 1, pp. 74-83.

Rodríguez-Escobar, J.A., Gonzalez-Benito, J. and Martínez-Lorente, A.R. (2006), "An analysis of the degree of small companies' dissatisfaction with ISO 9000 certification", *Total Quality Management & Business Excellence*, Vol. 17 No. 4, pp. 507-21.

Saint-Germain, R. (2005), "Information security management best practice based on ISO/IEC 17799", *Information Management Journal*, Vol. 39 No. 4, pp. 60-6.

Shewhart, W.A. (1939), *Statistical Method from the Viewpoint of Quality Control* (out of print: most recent edition: 1987, Dover Publications).

von Solms, B. and von Solms, R. (2005), "From information security to … business security", *Computers & Security*, Vol. 24 No. 4, pp. 271-3.

Further reading

Gillies, A.C. (2008), "The legal and ethical changes in the NHS landscape accompanying the policy shift from paper-based health records to electronic health records", *Studies in Ethics, Law and Technology*, Vol. 2 No. 1, p. 4.

Humphrey, W.S. (1987), "Characterising the software process: a maturity framework", Software Engineering Institute, CMU/SEI-87-TR-11, DTIC Number ADA182895.

About the author

Alan Gillies has been Professor of Information Management at the University of Central Lancashire since 1994 and a Fellow of the British Computing Society since 2004. He is the author of 20 books and 30 academic journal articles. He graduated from The Queen's College, Oxford in 1984 in Chemistry. His PhD, probably the first to be awarded by the University of Central Lancashire after gaining its charter in 1992, was in problem-solving methodology using KBS and formed the basis of his first book *The Integration of Expert Systems into Mainstream Software*. His second book, *Software Quality Theory and Management* is still in print in South East Asia 18 years after first publication. In 2009, he was appointed editor of the Emerald journal, *Clinical Governance: An International Journal*.