The Similarity between ISO 9001 and BS 7799-2

By Dr. David Brewer and Dr. Michael Nash, Gamma Secure Systems Limited

Introduction

Annex C to BS 7799-2:2002 [1] describes the similarities between it and other management system standards that conform to ISO Guide 72 [2]. One of these is ISO 9001 [3]. However, we believe that the correspondence is far closer than previously thought. This is an important conclusion for those organisations that are considering creating an integrated management system (MS), i.e., a single MS that complies with more than one management system standard.

In this paper we describe BS 7799-2:2002 in terms of a "PDCA" framework and an "SOA". PDCA stands for Plan-Do-Check-Act, also known as the Deming cycle, and is the overall framework required by [2]. SOA stands for Statement of Applicability, and is a list of information security controls that may, or may not, be applicable to an organisation. It was adopted in the first edition (1999) of the standard as a way of linking to the existing code of practice (BS 7799-1) that the new standard was designed to assess. We then describe the structure of ISO 9001, and explain how it can be recast to correspond exactly with the BS 7799-2:2002 structure. In our conclusion we draw upon a case study organisation that has an integrated MS, certified against both standards, that has applied the concepts described in this paper successfully.

BS 7799-2:2002

BS 7799-2:2002 is a specification for an Information Security Management System (ISMS). It is shortly to be upgraded to the status of a full International Standard, and published as ISO/IEC 27001. The normative part of this standard has four sections and an annex (Annex A). The requirements of the four sections are associated with the PDCA cycle as shown in Table 1. The annex defines all the controls that must be considered for generating the SOA. Thus the structure of BS 7799-2:2002, as will be ISO/IEC 27001, can be simply described as:

- A PDCA framework;
- An SOA.

ISO 9001:2000

ISO 9001:2000 is a specification for a Quality Management System (QMS). The normative part of this standard has five normative sections, numbered 4 – 8. All of these requirements must be met in order to claim conformance with the standard, save for section 7 (Product Realisation), where the standard states in paragraph 1.2 "Where exclusions are made, claims of conformity to this International Standard are not acceptable unless these exclusions are limited to requirements within clause 7, and such exclusions do not affect the organisation's ability, or responsibility, to provide product that meets customer and applicable regulatory requirements".

In Table 2 we relate the requirements of sections 4, 5, 6 and 8 to the PDCA framework. We treat section 7 as an SOA.

Treatment of Section 7 as an SOA

The BS 7799-2:2002 standard gives instruction on how the controls documented in BS 7799-2 Annex A are to be determined as being applicable or non-applicable. In particular, if the control is applicable

Section	Title	Association with PDCA cycle
4.1	General requirements	All
4.2.1	Establish the ISMS	PLAN
4.2.2	Implement and operate the ISMS	DO
4.2.3	Monitor and review the ISMS	CHECK
4.2.4	Maintain and improve the ISMS	ACT
4.3	Documentation requirements	All
5.1	Management commitment	All
5.2	Resource management	DO
6	Management review of the ISMS	CHECK
7	ISMS improvement	ACT

Table 1: Association of BS 7799-2:2002 requirements with the PDCA cycle

it must be justified in terms of the results of a risk assessment.

The controls listed in Section 7 of ISO 9001 may be excluded with justification. Thus, Section 7 of ISO 9001 may be treated in exactly the same manner as BS 7799-2 Annex A provided that applicable quality controls are also justified by reference to a risk assessment. Conversely for an integrated MS, information security controls that are declared to be non-applicable should also be justified as not applicable by reference to a risk assessment, in order to bring the two standards into line. Interestingly, this requirement was present in BS 7799-2:1999 but was dropped in the 2002 revision.

The amalgamation of these two approaches in an integrated MS should not be seen as a disadvantage. The justification of non-applicable information security controls greatly simplifies the task of determining, given a change of threat or business practice, whether a non-applicable control has now become applicable. The justification of Product Realisation controls by way of a reference to a risk assessment serves to remind us that, for many organisations, quality controls are not uniform across the whole organisation but are commensurate with the degree of risk involved. For example, in the software business, a fixed price assignment with tight timescales to produce a bespoke software system has a greater risk than a time and materials contract to supply programming staff, and the quality controls applied to management planning and reporting of the two projects would be very different.

A Common PDCA Framework

Table 3 shows the results of combining Tables 1 and 2. Table 3 has been ordered on "association with PDCA cycle" and "title". The table demonstrates that is it possible to amalgamate the requirements of the two standards into a common PDCA framework, given that the Product Realisation requirements of ISO 9001 are treated as an SOA. Thus, the structure of both standards can be described as:

- A PDCA framework;
- An SOA for information security
- An SOA for quality.

Section	Title	Association with PDCA cycle
4.1	General requirements	All
4.2.1	Documentation requirements (general)	All
4.2.2	Quality manual	PLAN
4.2.3	Control of documentation	All
4.2.4	Control of records	All
5.1	Management commitment	All
5.2	Customer focus	PLAN
5.3	Quality policy	PLAN
5.4	Planning	PLAN
5.5	Responsibility, authority and communication	All
5.6	Management review	CHECK
6.1	Provision of resources	DO
6.2	Human resources	DO
6.3	Infrastructure	PLAN
6.4	Work environment	PLAN
8.1	Measurement, analysis and improvement (general)	All
8.2	Monitoring and measurement	CHECK
8.3	Control of noncomforming product	DO
8.4	Analysis of data	CHECK
8.5	Improvement	ACT

Table 2: Association of ISO 9001:2000 requirements with the PDCA cycle

Case Study

Proof of any theoretical analysis as presented above can be demonstrated by its practical application. In this case we have applied the concept to our own MS.

Gamma's MS is an integrated MS, which is certified to both ISO 9001 and BS 7799-2. Certification to ISO 9001 was achieved first. Originally a paper based system conformant to ISO 9001:1994, we recast it as an electronic hypertext based system as part of the transition process from ISO 9001:1994 to ISO 9001:2000. Certification to

Association with PDCA cycle	Standard	Section	Title
All	7799-2	4.1	General requirements
	9001	4.1	
	7799-2	4.3	Documentation requirements covering control of documentation and control of records
	9001	4.2.1	
	9001	4.2.3	
	9001	4.2.4	
	7799-2	5.1	Management commitment
	9001	5.1	
	9001	8.1	Measurement, analysis and improvement (general)
	9001	5.5	Responsibility, authority and communication
PLAN	9001	5.2	Customer focus
	7799-2	4.2.1	Establish the ISMS (covers policy and risk analysis)
	9001	6.3	Infrastructure
	9001	5.4	Planning
	9001	4.2.2	Quality manual
	9001	5.3	Quality policy
	9001	6.4	Work environment
DO	9001	8.3	Control of noncomforming product
	9001	6.2	Human resources
	7799-2	4.2.2	Implement and operate the ISMS
	9001	6.1	Provision of resources
	7799-2	5.2	Resource management
CHECK	9001	8.4	Analysis of data
	9001	5.6	Management review
	7799-2	6	
	7799-2	4.2.3	Monitor and review the ISMS
	9001	8.2	Monitoring and measurement
ACT	9001	8.5	Improvement
	7799-2	4.2.4	
	7799-2	7	

Table 3: The common PDCA framework

ISO 9001:2000 was achieved in November 2002. In March 2004 we took the decision to augment the MS to comply with BS 7799-2. This was a straightforward exercise and we achieved certification to BS 7799-2 in July 2004. However, although we were able to expand existing quality practices (e.g. internal audit and management system reviews) to cover information security, there was inelegance in the asymmetric treatment of other requirements (e.g. the SOA and Product Realisation exclusions). Moreover, the resulting integrated MS was harder to navigate.

In July 2005, we applied the concepts presented in this paper to our integrated management system with the result that our implementation of both standards now conforms to a common PCDA framework. It is far easier to navigate and use, and, we anticipate, easier to expand.

Within Gamma, we manage risks through the use of Risk Treatment Plans (RTPs). These are a widely used process approach, originally documented in Australasian Standard AS/NZS 4360, Risk Management [5], and subsequently adopted by BS 7799-2. RTPs are used by many organisations in their implementation of risk-based management systems. With regards to the treatment of ISO 9001 section 7 as an SOA, we therefore created a single new RTP, titled "Unacceptable Quality", which facilitated the justification of our applicable Product Realisation requirements. This RTP has five risk statements (see [4]), which can briefly be described as follows:

- Failure to understand the client's requirement leading to a good chance that the company will create the wrong product;
- Inability to create the right product, even though the requirements are understood, because the company does not have the capability to produce it;
- Failure of the development and production processes;
- Having built the right product, delivery of something else;
- The fallback position in case that all the above referenced controls fail.

There is nothing new about the contents of this RTP. These risks have been identified and managed as part of our quality management system since ISO 9001:1994. All that was new was bringing them together into a single RTP. There

was no actual change to our existing management processes.

Summary and Conclusions

In this paper we have proposed that the structure of an integrated MS, conformant to ISO 9001 and BS 7999-2, can be described in terms of a common PDCA framework, an SOA for information security and an SOA for quality.

We have applied the concept to our own integrated MS and have found it to work extremely well in practice.

Comparison of Tables 1 and 2 reveals that the structure of BS 7799-2 is closely aligned to the concept of having a PDCA framework and an SOA. The structure of ISO 9001 is less well aligned and requires significant reorganisation to achieve alignment. Organisations that have existing ISO 9001 certifications and seek to achieve BS 7799-2 certification within a single integrated MS are advised to follow a similar structure to that presented in Table 3, in order to minimise transition costs and achieve the maximum benefits from integration.

References

[1] "Information security management systems - Specification with guidance for use", BS 7799-2:2002, British Standards Institution

[2] "Guidelines for the justification and development of management system standards", ISO Guide 72:2001

[3] "Quality management systems – Requirements", BS EN ISO 9001:2000

[4] "Measuring the effectiveness of an internal control system", Brewer, D.F.C., List, W., March 2004, http://www.gammassl.co.uk/topics/time

[5] AS/NZS 4360, Risk Management. Published by the Standards Association of Australia.

About the Authors

Dr. Michael Nash

Dr. David Brewer (right) has been involved in information security since he left university, and is an internationally recognised consultant in that subject. He was part of the team who created the ITSEC and the Common Criteria, and has worked for a wide range of government departments and commercial organisations both at home and abroad. He was one of the driving forces behind the Part 2 ISMS standard, has provided training in implementing ISO/IEC 17799 and has assisted many clients to build ISMSs since 1998 in Europe, East Africa, the Middle East and the Far East.

Dr. David Brewer

Dr. Michael Nash has a long background in information security. His first involvement came in 1985, working initially within NATO using the US TCSEC "Orange Book", and then setting up and managing the first UK security evaluation facility. He helped develop the UK national criteria, the ITSEC and finally the Common Criteria. On the other side, he has advised many major vendors and user organisations how to implement and improve information security, through the use of BS 7799 and related techniques. He has been involved in international standardisation for more than fifteen years, most recently as the Project Editor for the Guide to the Development of Protection Profiles and Security Targets, ISO/IEC TR 15292.