Similitud entre ISO 9001 y BS 7799-2

Por Dr. David Brewer y Dr. Michael Nash, Gamma Secure Systems Limited

Introducción

El Anexo C de BS 7799-2:2002 [1] describe las similitudes entre dicha norma y otros estándares de sistemas de gestión que se ajustan a la Guía ISO 72 [2]. Uno de ellos es ISO 9001 [3]. Sin embargo, creemos que la correspondencia es mucho más próxima de lo inicialmente pensado. Esta es una conclusión importante para aquellas organizaciones que están considerando la creación de un sistema de gestión (SG) integrado, p. ej., un único SG que cumpla con más de una norma de sistemas de gestión.

En este documento, describimos BS 7799-2:2002 en términos de un marco "PDCA" y un "SOA". PDCA significa Plan-Do-Check-Act [Planificar-Hacer-Verificar-Actuar], también conocido como ciclo Deming, y es el marco global requerido por [2]. SOA significa Statement of Applicability [declaración de aplicabilidad] y es una lista de controles de seguridad de la información que pueden ser, o no, aplicables a una organización. Fue adoptado en la primera edición (1999) del estándar como un modo de enlazar con el código de prácticas ya existente que el nuevo estándar estaba diseñado para evaluar. Después, describimos la estructura de ISO 9001 y explicamos cómo puede ser refundida para que se corresponda exactamente con la estructura de BS 7799-2:2002. En nuestra conclusión, recurrimos a un caso de estudio de una organización con un SG integrado, certificado en ambos estándares, que ha aplicado con éxito los conceptos descritos en este documento.

BS 7799-2:2002

BS 7799-2:2002 es una especificación de un Sistema de Gestión de la Seguridad de la Información (SGSI). En breve, será promovida a la condición plena de Estándar Internacional y será publicada como ISO/IEC 27001 [N. del T.: este artículo se publicó originalmente antes de Octubre de 2005, fecha de aparición de ISO/IEC 27001]. La parte normativa de este estándar tiene cuatro secciones y un anexo (Anexo A). Los requisitos de las cuatro secciones están asociados al ciclo PDCA en la forma mostrada en la Tabla 1. El anexo define todos los controles que deben ser considerados para generar el SOA. Por tanto, la estructura de BS 7799-2:2002, al igual que la de la futura ISO/IEC 27001, puede ser descrita sencillamente como:

- Un marco PDCA.
- Un SOA.

ISO 9001:2000

ISO 9001:2000 es una especificación de un Sistema de Gestión de la Calidad (SGC). La parte normativa de este estándar tiene cinco secciones, numeradas del 4 al 8. Se deben satisfacer todos estos requisitos para acreditar la conformidad con la norma, a excepción de la sección 7 (Realización del Producto), donde el estándar estipula en su cláusula 1.2: "Cuando se realicen exclusiones, no se podrá alegar conformidad con esta norma a menos que dichas exclusiones queden restringidas a los requisitos expresados en el capítulo 7 y que tales exclusiones no afecten a la capacidad o responsabilidad de la organización para proporcionar productos que cumplan con los requisitos del cliente y los reglamentarios aplicables".

En la tabla 2, relacionamos los requisitos de las secciones 4, 5, 6 y 8 con el marco PDCA. Tratamos la sección 7 como un SOA.

Tratamiento de la Sección 7 como SOA

El estándar BS 7799-2:2002 indica cómo los controles documentados en el anexo A de BS 7799-2 han de

Sección	Título	Asociación con ciclo PDCA
4.1	Requerimientos generales	Todos
4.2.1	Establecer el SGSI	PLANIFICAR [P]
4.2.2	Implementar y utilizar el SGSI	HACER [D]
4.2.3	Monitorizar y revisar el SGSI	VERIFICAR [C]
4.2.4	Mantener y mejorar el SGSI	ACTUAR [A]
4.3	Requerimientos de documentación	Todos
5.1	Compromiso de la Dirección	Todos
5.2	Gestión de recursos	HACER [D]
6	Revisión del SGSI por la Dirección	VERIFICAR [C]
7	Mejora del SGSI	ACTUAR [A]

Tabla 1: Asociación de los requisitos de BS 7799-2:2002 con el ciclo PDCA

ser determinados como aplicables o no. En concreto, si el control es aplicable, debe ser justificado en relación a los resultados de una evaluación de riesgos.

Los controles enumerados en la Sección 7 de ISO 9001 pueden ser excluidos con la correspondiente justificación. Por tanto, la Sección 7 de ISO 9001 puede ser tratada exactamente del mismo modo que el Anexo A de BS 7799-2, siempre que los controles de calidad aplicables también se justifiquen en relación a una evaluación de riesgos. A la inversa, para un SG integrado, los controles de seguridad de la información que sean declarados como no aplicables, también deberían ser justificados en relación a una evaluación de riesgos, con objeto de alinear los dos estándares. Curiosamente, este requisito fue presentado en BS 7799-2:1999 pero se retiró en la revisión de 2002.

La fusión de estos dos enfoques en un SG integrado no debería verse como una desventaja. La justificación de los controles de seguridad de la información no aplicables simplifica enormemente la tarea de determinar, ante un cambio en las amenazas o en las prácticas de negocio, si un control no aplicable se ha convertido en aplicable. La justificación de los controles de la Realización del Producto por medio de una referencia a una evaluación de riesgos sirve para recordarnos que, para muchas organizaciones, los controles de calidad no son uniformes a lo largo de las mismas sino que son proporcionales al grado de riesgo implícito. P. ej., en el sector del software, un encargo a precio cerrado con plazos ajustados para realizar un sistema de software a medida implica un riesgo mayor que un contrato en base a tiempo y materiales para suministrar programadores, y los controles de calidad aplicados a la planificación e informes de gestión de ambos proyectos serían muy diferentes.

Un marco PDCA común

La Tabla 3 muestra el resultado de combinar las Tablas 1 y 2. La Tabla 3 ha sido ordenada según "asociación con ciclo PDCA" y "título". La tabla demuestra que es posible fusionar los requisitos de las dos normas en un marco PDCA común, siempre y cuando los requisitos para la Realización del Producto de ISO 9001 sean tratados como un SOA. Por tanto, la estructura de ambos estándares puede describirse como:

- Un marco PDCA.
- Un SOA para la información de la seguridad.
- Un SOA para la calidad.

Sección	Título	Asociación con ciclo PDCA
4.1	Requisitos generales	Todos
4.2.1	Requisitos de la documentación (generalidades)	Todos
4.2.2	Manual de calidad	PLANIFICAR [P]
4.2.3	Control de los documentos	Todos
4.2.4	Control de los registros	Todos
5.1	Compromiso de la Dirección	Todos
5.2	Enfoque al cliente	PLANIFICAR [P]
5.3	Política de la calidad	PLANIFICAR [P]
5.4	Planificación	PLANIFICAR [P]
5.5	Responsabilidad, autoridad y comunicación	Todos
5.6	Revisión por la Dirección	VERIFICAR [C]
6.1	Provisión de recursos	HACER [D]
6.2	Recursos humanos	HACER [D]
6.3	Infraestructura	PLANIFICAR [P]
6.4	Ambiente de trabajo	PLANIFICAR [P]
8.1	Medición, análisis y mejora (generalidades)	Todos
8.2	Seguimiento y medición	VERIFICAR [C]
8.3	Control del producto no conforme	HACER [D]
8.4	Análisis de datos	VERIFICAR [C]
8.5	Mejora	ACTUAR [A]

Tabla 2: Asociación de los requisitos de ISO 9001:2000 con el ciclo PDCA

Caso de Estudio

La prueba de un análisis teórico como el presentado anteriormente puede ser demostrada mediante su aplicación práctica. En este caso hemos aplicado el concepto a nuestro propio SG.

El SG de Gamma es un SG integrado, certificado tanto en ISO 9001 como en BS 7799-2. La certificación en ISO 9001 fue lograda en primer lugar.

Similitud entre ISO 9001 y BS 7799-2

Asociación con ciclo PDCA	Norma	Sección	Título
Todos	7799-2	4.1	Requisitos generales
	9001	4.1	
	7799-2	4.3	Requisitos de documentación relativos al control de la documentación y el control de registros
	9001	4.2.1	
	9001	4.2.3	
	9001	4.2.4	
	7799-2	5.1	Compromiso de la Dirección
	9001	5.1	
	9001	8.1	Medición, análisis y mejora (generalidades)
	9001	5.5	Responsabilidad, autoridad y comunicación
PLANIFICAR [P]	9001	5.2	Enfoque al cliente
	7799-2	4.2.1	Establecer el SGSI (cubre política y análisis de riesgos)
	9001	6.3	Infraestructura
	9001	5.4	Planificación
	9001	4.2.2	Manual de calidad
	9001	5.3	Política de la calidad
	9001	6.4	Ambiente de trabajo
HACER [D]	9001	8.3	Control del producto no conforme
	9001	6.2	Recursos humanos
	7799-2	4.2.2	Implementar y utilizar el SGSI
	9001	6.1	Provisión de recursos
	7799-2	5.2	Gestión de recursos
VERIFICAR [C]	9001	8.4	Análisis de datos
	9001	5.6	Revisión por la Dirección
	7799-2	6	
	7799-2	4.2.3	Monitorizar y revisar el SGSI
	9001	8.2	Seguimiento y medición
ACTUAR [A]	9001	8.5	Mejora
	7799-2	4.2.4	
	7799-2	7	

Tabla 3: El marco PDCA común

El sistema original basado en papel y conforme a ISO 9001:1994 lo reconvertimos a un sistema electrónico basado en hiperenlaces como parte del proceso de transición de ISO 9001:1994 a ISO 9001:2000. La certificación en ISO 9001:2000 fue lograda en Noviembre de 2002. En Marzo de 2004, tomamos la decisión de aumentar el SG para cumplir con BS 7799-2. Esto fue una implantación sencilla y logramos la certificación en BS 7799-2 en Julio de 2004. Sin embargo, a pesar de que fuimos capaces de ampliar nuestras prácticas de calidad existentes (p. ej., auditoría interna y revisiones del sistema de gestión) para cubrir la seguridad de la información, resultaba poco elegante en el tratamiento asimétrico de otros requisitos (p. ej., el SOA y exclusiones de la Realización del Producto). Además, el SG integrado resultante era más difícil de navegar.

En Julio de 2005, aplicamos los conceptos presentados en este documento a nuestro sistema de gestión integrado, obteniendo como resultado una implantación de ambas normas conforme a un marco PDCA común. Resulta mucho más sencillo de navegar y utilizar y, como esperábamos, más fácil de ampliar.

En Gamma, gestionamos los riesgos mediante el uso de Planes de Tratamiento del Riesgo (Risk Treatment Plans, RTPs). Estos son un enfoque de procesos ampliamente difundido y originalmente documentado en el Australasian Standard AS/NZS 4360, Risk Management [5], y posteriormente adoptados por BS 7799-2. Los RTPs son utilizados por muchas organizaciones para la implantación de sistemas de gestión en base al riesgo. Respecto al tratamiento de la Sección 7 de ISO 9001 como un SOA, creamos un único y nuevo RTP titulado “Calidad Inaceptable”, que facilitó la justificación de nuestros requisitos aplicables para la Realización del Producto. Este RTP tiene cinco declaraciones de riesgo (véase [4]), que pueden ser descritas brevemente de la siguiente forma:

- La falta de entendimiento de las necesidades del cliente conduce a tener muchas probabilidades de que la compañía cree el producto equivocado.
- Incapacidad de crear el producto adecuado, incluso cuando los requisitos son bien entendidos, porque la compañía no dispone de las habilidades para producirlo.
- Fallo de los procesos de desarrollo y producción.
- Habiendo elaborado el producto correcto, se entrega otra cosa.
- La alternativa en caso de que todos los controles anteriormente indicados fallen.

No existe nada nuevo en los contenidos de este RTP. Estos riesgos han sido identificados y gestionados como parte de nuestro sistema de gestión de la calidad desde ISO 9001:1994. La única novedad fue integrarlos todos en un único RTP. No hubo un cambio real en nuestros procesos de gestión ya existentes.

Sumario y Conclusiones

En este documento hemos propuesto que la estructura de un SG integrado, conforme a ISO 9001 y a BS 7799-2, puede ser descrita en función de un marco común PDCA, un SOA para la seguridad de la información y un SOA para la calidad.

Hemos aplicado el concepto a nuestro propio SG integrado y hemos encontrado que funciona sumamente bien en la práctica.

La comparación de las Tablas 1 y 2 revela que la estructura de BS 7799-2 está íntimamente alineada con el concepto de tener un marco PDCA y un SOA. La estructura de ISO 9001 no está tan bien alineada y requiere de una reorganización significativa para lograr el alineamiento. Para las organizaciones que dispongan de certificación en ISO 9001 y busquen obtener la certificación en BS 7799-2 con un único SG integrado, se aconseja seguir una estructura similar a la presentada en la Tabla 3, con objeto de minimizar los costes de transición y lograr los máximos beneficios de la integración.

Referencias

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

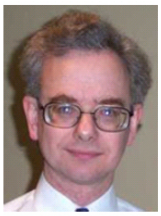
[2] “Guidelines for the justification and development of management system standards”, ISO Guide 72:2001.

[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., Marzo de 2004, http://www.gammassl.co.uk/topics/time

[5] AS/NZS 4360, Risk Management. Publicado por la Standards Association of Australia.

Acerca de los Autores



Dr. Michael Nash

El Dr. David Brewer (derecha) lleva involucrado en la seguridad de la información desde que dejó la universidad y es un consultor internacionalmente reconocido en este tema. Formó parte del equipo que creó ITSEC y los Criterios Comunes y ha trabajado para un amplio número de organismos gubernamentales y organizaciones comerciales tanto en su país como en el exterior. Fue uno de impulsores de la Parte 2 del estándar SGSI, ha impartido formación en la implantación de ISO/IEC 17799 y ha asistido a muchos clientes en la construcción de sus SGSI desde 1998 en Europa, África Oriental, Oriente Medio y Lejano Oriente.

Dr. David Brewer

El Dr. Michael Nash tiene amplia experiencia en seguridad de la información. Su primera implicación tuvo lugar en 1985, trabajando inicialmente en la OTAN en la utilización del US TCSEC “Orange Book” y estableciendo y gestionando el primer recurso de evaluación de la seguridad en el Reino Unido. Colaboró en el desarrollo de un criterio de ámbito nacional en el Reino Unido, el ITSEC y, finalmente, los Criterios Comunes. Por otro lado, ha asesorado a muchas grandes empresas y organizaciones de usuarios en cómo implantar y mejorar la seguridad de la información, mediante el uso de BS 7799 y técnicas relacionadas. Ha estado implicado en la estandarización internacional durante más de quince años y, más recientemente, como editor del proyecto para la “Guide to the Development of Protection Profiles and Security Targets, ISO/IEC TR 15292”.

[Traducción del original inglés por Agustín López Neira y Javier Ruiz Spohr, www.iso27000.es]
[Translated from English original by Agustín López Neira and Javier Ruiz Spohr, www.iso27000.es]