1.- Una buena gestión de riesgos identifica éstos antes de que se materialicen, de manera que se puedan evitar o, en caso de que sean inevitables, se puedan definir las medidas que minimizarán su impacto en caso de que se produzcan. ¿Qué acciones proactivas se proponen en tu propuesta de proyecto para implantar ISO27001 y PCI para la detección de riesgos?

De la determinación de la SOA en las fases iniciales de la implantación se desprende la necesidad de realizar un análisis de riesgos, uno de los pasos iniciales en la implantación, en el punto 6.1.2 Valoración de los Riesgos de la seguridad de la información apartado (a) se establece la necesidad no sólo de determinar los criterios de valoración de riesgos sino de mantenerlos mediante un plan de tratamiento de riesgos (6.1.3.b Tratamiento de riesgos de la seguridad de la información), asimismo en el punto 8.2 Valoración de riesgos de la seguridad de la información se insta a la organización a realizar el análisis de riesgos y realizarlo a intervalos planificados.

Por todo ello en los puntos 3.11.2 y 3.6.2a del trabajo Determinar el grado de aplicabilidad y Consideraciones respecto a la gestión de riesgos recomiendo que la gestión de riesgos y la SOA se realicen de forma semestral y que el resultado de la misma se traspase al SGSI para realizar las acciones, recursos y plazo en su gestión. Consciente de la importancia de la gestión de riesgos recomiendo que en vez de realizarse anualmente –como es habitual- la gestión de riesgos y la SOA se realicen semestralmente. Finalmente en el punto 11.1 Factores Clave de Éxito remarco la importancia de disponer de gestión del riesgo implementada según lo dicho anteriormente.

2.- Es habitual en la gestión de la seguridad que aunque la dirección de la organización entienda que su objetivo sea organizar la captura, almacenamiento, manipulación, procesamiento y gestión de los datos y servicios, de tal manera que se satisfagan los requerimientos de negocio en cuanto a su integridad, confidencialidad y disponibilidad; esponsorice de manera inicial el proyecto de certificación en ISO27001 o PCI; pero que, a medida que el proyecto avanza, planteen aspectos como el elevado coste de implementación y mantenimiento, que no se puede proteger contra todas las amenazas, que los niveles de los objetivos establecidos son demasiado altos y chocan frontalmente con objetivos de negocio; o hasta que acaben tomando la "actitud del avestruz" y no se acaben adoptando los niveles requeridos después de los cambios. ¿Qué medidas planteas para éstas situaciones?

Estas situaciones suceden y el consultor debe estar preparado para ello, en el trabajo hago énfasis en la R2 Identificar al sponsor de la necesidad de contar con el máximo sponsor posible de forma que la implantación forme parte de los objetivos de la empresa, por otra parte la “actitud del avestruz” viene motivada en gran parte por un alcance que la empresa no pueda asumir, de ahí que el R3 Determinar el alcance haya añadido la necesidad fundamental de tener un alcance alineado con el sponsor como garantía de éxito y de no abandono (sea asequible). Así en el punto 7.4 Problemas posibles recomiendo que ante una Imposibilidad de Acción (7.4.2) o bien una Falta de Presupuesto (7.4.3) dichas casuísticas sean detectadas lo antes posible y gestionadas

mediante el establecimiento de acciones asumibles que impida el abandono del proyecto. Dichas situaciones debieran ser detectadas por la gestión del riesgo ya comentada en la pregunta anterior.

Hay que entender que la motivación de certificación suele ser por motivos de negocio, generalmente una empresa se certifica por la necesidad de acreditarse para acceder a un contrato que exige su certificación (ISO27001) en el caso de PCI es necesario por el riesgo de multas (pueden ser millonarias) que la propia PCI puede imponer en caso de investigación así como la necesidad de demostrar diligencia debida en la gestión de los datos del CDE, por tanto ambas situaciones pueden pasar pero con un alcance bien definido, el mejor sponsor posible y la "amenaza" de multas cuantiosas o la pérdida de clientes bien gestionada pueden ayudar a proseguir con el proyecto.

3.- Todo proyecto tiene la necesidad de medir y sobretodo en la fase de implementación, para asegurarnos que estamos siguiendo el camino correcto (lo que no se puede medir, no se puede gestionar, controlar, ni mejorar). Comenta tres indicadores que siempre puedas encontrar en éste tipo de proyectos, indicando: Descripción, objetivo y método de cálculo de cada uno de ellos.

Hay infinidad así como según se haya planificado la implantación surgen más, de sistemas en fases de implantación, y aquí abro un paréntesis, como implantador los indicadores de proyecto como Hitos completados a tiempo y Desviación de esfuerzo frente a planificación son a mi juicio menos importantes, un buen consultor debería no fijarse tanto en indicadores y más en el cambio organizacional que produce su esfuerzo, desde luego el proyecto debe ser rentable pero aportaremos más valor al negocio si nos ve como un aliado que se esfuerza y sacrifica con la empresa que como un consultor clásico con el cronómetro en la mano. La experiencia y el buen hacer deben producir tiempo de calidad que evite rework y cuyos entregables tengan ciclos de aceptación en el cliente muy cortos por ser de gran calidad.

Con el sistema en fases iniciales de implantación remarcaría los siguientes:

Nombre	% Controles de la SOA implantados
Polaridad	Mayor es mejor
Método de cálculo	$\left(\frac{\text{Número de controles aplicables implantados}}{\text{Total controles aplicables}}\right) * 100$ Nota: la SOA tiene 114 controles Nota: se hace el mismo para los controles PCI
Periodicidad	Semestral
Nombre	% Riesgos para los que se han implantado controles satisfactorios

Polaridad	Mayor es mejor
Método de cálculo	$\left(\frac{\text{Número de riesgos con controles implantados}}{\text{número de riesgos detectados}}\right) * 100$
Periodicidad	Semestral
Nombre	% trabajadores involucrados en las políticas de Seguridad
Polaridad	Mayor es mejor
Método de cálculo	$\left(\frac{\text{Número de trabajadores formados en seguridad}}{\text{número de trabajadores}}\right) * 100$ Nota: se hace el mismo para proveedores
Periodicidad	Semestral
Nombre	% Incidentes de seguridad detectados resueltos
Polaridad	Mayor es mejor
Método de cálculo	$\left(\frac{\text{Número de incidentes de seguridad tratados}}{\text{Número de incidentes de seguridad detectados}}\right) * 100$
Periodicidad	Semestral
Nombre	% Clientes satisfechos
Polaridad	Mayor es mejor Nota: es un objetivo de seguridad-viabilidad del proyecto fijar objetivos cualitativos además de los cuantitativos, cada empresa indica qué desea, si % o número (por ejemplo queremos obtener un 7/10, este año y aumentar para el año que viene a 8, 9 … o bien queremos obtener un 90% de clientes satisfechos)
Método de cálculo	$\left(\frac{\sum Respuestas\ pregunta\ Satisfaccion}{Encuestas\ recibidas}\right)$
Periodicidad	Anual (al iniciar la implantación realizar la primera como estrategia de marketing hacia los clientes, el mensaje es: “estamos mejorando y queremos mejorar más, esto hará que el servicio que te prestamos también mejore, y lo hacemos sin que nos lo pidas (y lo pagues)”
Nombre	Número de acciones de mejora continua emprendidas
Polaridad	Mayor es mejor
Método de cálculo	$\left(\frac{\text{Número de acciones de mejora completadas}}{\text{Número deacciones identificadas}}\right) * 100$

Periodicidad	Semestral El propósito de mejora continua es fundamental en un sistema de calidad, es nuestra responsabilidad impulsarlo y motivar a la empresa a seguirlo con diligencia, es de más alto nivel pero también una excelente palanca de cambio para aprovechar el impulso certificador para emprender cambios y dar la oportunidad a la plantilla de expresar su opinión

Como nota final me gustaría añadir que el pasado 21 de Junio 2016 tuve la oportunidad de presentar el compendio de mejores prácticas de implantación ISO27001:2013 (como derivada del presente trabajo) en la UPC esponsorizado por el itSMF (http://www.meetup.com/es/itSMF-CAT/events/231559715/) os adjunto la PPT en la que expliqué la implantación de la norma basándome en las mejores prácticas que practiqué con la TFC, me hubiera encantado ponerla pero por limitaciones de espacio no me cabía en el trabajo y tuve que cortar varios apartados entre los que se encontraba este.

Muchas gracias y un saludo