INFORME TÉCNICO

La aplicación del enfoque basado en el riesgo en ISO 9001: 2015

Autores Colaboradores:
David J White, Consultor Senior, SAI Global

Introducción

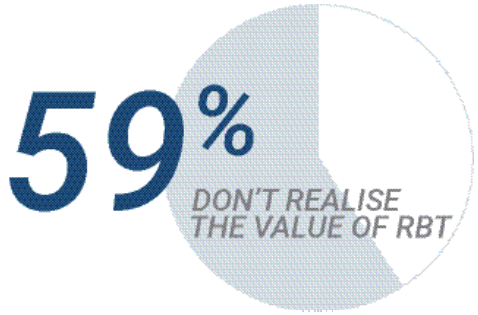
Una organización que incorpore eficazmente el Enfoque basado en el riesgo (RBT sus siglas en inglés) será más capaz de gestionar y hacer frente a la incertidumbre y sus posibles consecuencias negativas. También mejorará su capacidad para identificar y explotar los beneficios empresariales que resultarán de una mejor gestión de las oportunidades definidas.

La ISO 9001 se basa en el ciclo de gestión plan-hacer-verificar-actuar (PHVA). Sugerimos que, al diseñar un sistema de gestión de calidad (SGC), las organizaciones consideren la combinación de los enfoques RBT y PHVA. Esto no solo garantizará la conformidad con la norma, sino que también es una vía para la mejora continua mediante la aplicación de medidas preventivas específicas para ofrecer mejores resultados.

intertek SAI GLOBAL

Mediante la identificación de riesgos clave, sus impactos negativos pueden evitarse o minimizarse. La identificación temprana hace que la gestión de riesgos sea más rápida, económica y eficaz. La alternativa, no hacer nada hasta que se produce un fracaso y luego experimentar una crisis, es más costosa y más peligrosa para el prestigio de la marca, negocio y calidad por igual.

Por lo tanto, sostenemos que adoptar el RBT tiene sentido para el negocio. En una encuesta reciente de un seminario web en vivo de SAI Global, el 41% de los participantes dijeron que aplican el RBT para mejorar su rendimiento general del negocio y el 35% dijo que sí porque es un requisito del cliente (gracias a la ISO 9001).



¿Cómo se integra el RBT en la ISO 9001?

La ISO 9000 define el **riesgo** como **"el efecto de la incertidumbre"**, por lo general en relación con el logro de un negocio planificado o esperado o expectativa del cliente, u objetivo de calidad. Aunque el riesgo suele considerarse negativo, la ISO 9001 también aborda los riesgos positivos (u "oportunidades"), por ejemplo, cuando un riesgo empresarial tiene una probabilidad baja y un alto potencial al alza.

Independientemente de si los problemas se determinan como riesgos u oportunidades, el enfoque PHVA en la ISO 9001 siempre debe aplicarse. Esto significa:

- Comprender la organización y su contexto (cláusula 4.1), que obliga a la organización a determinar las cuestiones internas y externas más relevantes para su propósito y dirección estratégica **(cláusula 5.1.1 b).**
- Comprender las necesidades y expectativas de los accionistas **(cláusula 4.2).**
- Determinar el alcance del sistema de gestión de calidad (SGC) **(cláusula 4.3 a & b).**
- Determinación y tratamiento de los riesgos a nivel de proceso **(cláusula 4.4.1 f).**
- Demostrar el compromiso de liderazgo promoviendo el RBT en la organización **(cláusula 5.1.1 d).**
- Planificación y adopción de medidas para hacer frente a los riesgos **(cláusula 6.1).**
- Gestión de otros cambios previstos en el SGC **(cláusula 6.3 a).**
- Revisar la eficacia de las medidas adoptadas para hacer frente a los riesgos **(cláusula 9.3.2 e).**
- Actualización de los riesgos originalmente determinados durante la planificación anterior **(cláusula 6.1),** en relación con:
    - cambios en el contexto de la organización **(cláusula 9.3.2 b).**
    - riesgos emergentes asociados con las acciones adoptadas en respuesta a cualquier inconformidad **(cláusula 10.2.1 e).**

Todos estos requisitos deben abordarse si la organización debe aplicar RBT de manera eficaz e implementar un enfoque PHVA estructurado para la gestión de riesgos.

¿Quién es el responsable del enfoque basado en el riesgo?

Idealmente, cada empleado debe tener cierta responsabilidad y obligación por el RBT. Dicho esto, la ISO 9001 hace hincapié en la importancia del liderazgo y el papel de la dirección. Dado que son responsables de los resultados y consecuencias generales del SGC, sin mencionar los objetivos y prioridades de la organización, la responsabilidad de la aplicación efectiva del RBT también debe residir en ellos.

EL PAPEL DE LA DIRECCIÓN

Cuando la dirección se enfrenta a desafíos externos o cambios internos, el RBT puede ayudar a garantizar que todos los riesgos relevantes sean considerados y respondidos cuando sea apropiado. Ejemplos de tales consideraciones incluyen:

- Nuevos requisitos reglamentarios o legales, por ejemplo, GDPR.
- Programas de contratación y despido.
- Gestión de ubicaciones y unidades operativas.
- Instalación de nuevas soluciones de seguridad de la información (SI) o tecnología de la información (TI).
- Objetivos significativos de mejora del margen.
- Entrar en los mercados con nuevos productos, o en nuevas geografías.
- Proyectos o contratos inusualmente grandes y complejos.
- Análisis de costos/beneficios de la cadena de suministro y opciones de externalización.
- Movimientos agresivos de la competencia.
- Aumento de las horas extras de trabajo.
- Ajustes a la baja de los presupuestos de formación.
- Equipos de envejecimiento u otras instalaciones/infraestructuras clave.
- Bajo rendimiento financiero.
- Desaceleraciones significativas en las condiciones del mercado.

Cualquiera de las anteriores puede considerarse una oportunidad con distintos grados de riesgo. O podrían ser considerados riesgos que (que en caso de ser reducidos) pueden ser oportunidades presentes. Por lo tanto, se debe aplicar el PBR, especialmente para la estrategia y la planificación.

Si bien la responsabilidad última de la promoción del RBT recae en la dirección, se puede delegar la responsabilidad de definir y gestionar riesgos específicos.

Una clave para el compromiso es asegurar que las personas sientan que sus contribuciones están ayudando a mejorar la organización. Al exigir a todos los empleados que adopten el RBT y capacitar a las personas autorizadas en todos los niveles definidos en el SGC, cada empleado puede vincular la forma en que gestionan sus tareas y riesgos con la forma en que la organización está logrando sus objetivos.

Es un pleonasmo de gestión que **"lo que se mide se gestiona"** y podemos ver que esto se aplica en el caso del RBT. **El enfoque basado en el riesgo** destaca los temas y problemas críticos que una organización debe abordar. También ayuda a una organización a entender lo bien que se está adaptando al cambio. Un enfoque probado y de mejores prácticas para gestionar y alcanzar cualquier objetivo es medir, evaluar y, en caso necesario, mejorar las acciones tomadas. Este enfoque es igualmente importante para la gestión de acciones en respuesta a riesgos y oportunidades específicos y en constante evolución.

A medida que se adopta el RBT en toda la organización, todas las personas con funciones de implementación, o algún grado de propiedad del proceso, tienen la responsabilidad de identificar los riesgos y oportunidades más importantes en su área. Estos deben gestionarse a través del SGC (mediante un enfoque PHVA), y la dirección debe ser responsable de los resultados finales.

¿Como aplicar e incorporar el enfoque Basado en el Riesgo?

Aunque es posible que los riesgos y las oportunidades nunca puedan ocurrir, determinar aquellos que son críticos para el negocio es una tarea importante para las organizaciones con un SGC moderno basado en la ISO 9001. La prioridad y el enfoque en los riesgos más importantes es la clave. La organización debe identificar y capacitar a las personas con la experiencia, el juicio y las habilidades técnicas para utilizar el RBT para determinar riesgos y oportunidades.

Otro factor clave en la aplicación efectiva del RBT, es que el liderazgo de la organización demuestre el compromiso y garantice que se proporcionan los sistemas y recursos necesarios para hacer el trabajo.

Aunque no es específicamente requerido por la ISO 9001, la incorporación del RBT en la política de calidad y el desarrollo de algún tipo de proceso de gestión de riesgos en el SGC (y asegurar que está sujeto a auditoría interna y revisión de la gestión) son formas probadas de promover la aplicación efectiva del RBT en toda la organización.

Una vez identificado el contexto de la organización (con sus desafíos internos y externos identificados) y entendidas las necesidades de los accionistas, **las cláusulas ISO 9001 6.1 y 4.4.1.f** requieren que **se determinen** y aborden los riesgos. La ISO 9000 define estos términos de esta manera:

- **Determinación:** actividad para conocer una o más características y su valor característico.
- **Riesgo:** efecto de incertidumbre.

El **efecto** puede considerarse como el grado o la gravedad del daño que resultaría si el riesgo realmente se produjera; **incertidumbre** puede considerarse como la probabilidad de que se produzca el riesgo.

En términos de la ISO 9001, la evaluación del efecto y la incertidumbre se consideraría suficiente a la hora de determinar los riesgos. Sin embargo, muchas organizaciones tienen en cuenta características adicionales a la hora de determinar los riesgos. El modelo de gravedad-acontecimiento-detección-acción (GADA) se utiliza a menudo en este sentido:

- **Gravedad:** el impacto potencial de un evento de riesgo (es decir, el tipo y la cantidad de daño).
- **Acontecimiento:** la probabilidad de que ocurra un evento de riesgo.
- **Detección:** ¿con qué rapidez la organización identificaría un acontecimiento?
- **Acción:** ¿qué tan rápido puede reaccionar la organización ante un acontecimiento y qué tan efectiva será su reacción?

Tanto la **detección como la acción** a menudo se tienen en cuenta al decidir qué respuesta de riesgo aplicar, especialmente si la decisión es **tolerar** un cierto nivel de riesgo. Esto hace que sea fundamental tener la capacidad de detectar y responder rápidamente a los riesgos.

Un modelo utilizado a menudo por las organizaciones para ayudarles a decidir qué **tipo de respuesta** hacer a un **riesgo conocido**, es tratamiento-transferencia-terminar-tolerar:

- **Tratamiento:** abordar el riesgo directamente, cambiar los procesos, añadir nuevos controles u otras medidas para reducir la incertidumbre y/o los efectos negativos a niveles aceptables, (por ejemplo, rojo a verde, alto a medio, 10 a 5).
- **Transferencia:** implica trasladar el problema internamente a otra zona más adecuada o externamente a una organización de 2a parte. Por ejemplo, la externalización de la gestión de los riesgos de ciberataques a una organización especializada en seguridad de TI.
- **Terminar:** esto significa esencialmente eliminar el riesgo, Un ejemplo de esto sería al cesar una actividad o proceso.
- **Tolerar:** esto depende de la capacidad de una organización para resistir y absorber eventos de riesgo. Al tomar esta decisión, una organización consciente habrá considerado su capacidad para detectar rápidamente el riesgo y estará dispuesta a responder para limitar cualquier daño.

Aunque la norma ISO 9001 no requiere específicamente tipos obligatorios de documentación, como un registro de riesgos o una base de datos, o procedimientos documentados de gestión de riesgos, la mayoría de las organizaciones de alto rendimiento que han adoptado el RBT, han optado por crear documentación para ayudar a su gestión de riesgos.

Casos prácticos de RBT-ineficaces frente a eficaces

Los siguientes ejemplos se basan en empresas del mundo real y sus prácticas de gestión de riesgos.

GESTIÓN DE RIESGO INEFICAZ – RBT NO UTILIZADO

Una gran organización multinacional de servicios con más de 65.000 clientes en 38 países había iniciado un programa global para reestructurar sus sistemas de TI, incluida la introducción de nuevos portales de clientes interactivos. El programa estaba previsto que tomara tres años, financiado con gastos de capital a un costo presupuestado de 3 millones de dólares americanos.

La organización utilizó su proceso establecido de selección de proveedores, estableció el contrato y acordó la especificación basada en una revisión interna por parte del equipo ejecutivo. El equipo ejecutivo, sin embargo, tenía poco conocimiento sobre la tecnología y no pudo evaluar correctamente la funcionalidad reclamada del software.

Una característica clave del contrato era que todos los datos e información transaccional del cliente se migrarían automáticamente del sistema antiguo al nuevo. Esto llevaría tres meses y ocurriría en el tercer año del proyecto. Se llevó a cabo un análisis de fortalezas-oportunidades-debilidades-amenazas (FODA), pero la migración de datos no se consideró un riesgo significativo, en gran parte gracias a las garantías verbales dadas por los arquitectos de TI. Los usuarios del sistema existente no estaban participando completamente en la fase de captura de requisitos de software (que se llevó a cabo por el proveedor de TI subcontratado).

No fue llevado a cabo ningún ensayo fuera de línea antes de que comenzara la migración completa de datos. El proceso falló realmente mal y resultó en daños significativos en los datos del cliente antes de que se detuviera. Los efectos incluyeron:

- Un retraso de 18 meses en el proyecto.
- Costos adicionales para el negocio de $900 mil dólares americanos.
- Insatisfacción significativa del cliente y la pérdida de tres cuentas clave por un valor total de $3.2 millones de dólares americanos.
- Un número significativo de clientes más pequeños también llevaron su negocio a otro lugar.
- Pérdida de muchos empleados clave para los competidores debido a los enormes niveles de insatisfacción de los empleados como resultado del alto nivel de perturbación en el lugar de trabajo, el aumento de las cargas de trabajo y el estrés causado por el hecho de que los datos de los clientes tuvieron que ser transferidos manualmente.

Unos cuatro años más tarde, esta compañía todavía se está recuperando. Su marca y prestigio profesional fueron enormemente dañados, lo que resultó en una pérdida significativa de negocios futuros. En este caso, es evidente que la empresa no logró:

- Determinar las posibles cuestiones internas relacionadas con esta oportunidad (cláusula 4.1).
- Realizar suficientes análisis de participación/necesidades de los accionistas (cláusula 4.2).
- Considerar los riesgos (cláusula 6.1) para el propio programa y/o para las operaciones comerciales como las operaciones habituales a medida que era ejecutado el programa.
- Evaluar eficazmente la capacidad del proveedor y gestionar el servicio externalizado (cláusula 8.4).

GESTION DE RIESGO EFECTIVA CON EL RBT

Esta empresa ha estado en el negocio durante 40 años, fabricando grandes motores eléctricos. Algunos empleados han estado en la organización durante 30 años o más, y están planeando retirarse pronto.

La empresa ha estado importando alambre de cobre eléctrico de alta calidad de dos proveedores principales, ambos en Asia. Han utilizado los mismos dos proveedores durante más de 10 años y aunque la calidad del cable de cobre suministrado se considera satisfactoria, ocasionalmente experimentan retrasos en la entrega. Estos afectan significativamente a la producción ya que la empresa no transporta grandes reservas de cobre, gracias a su alto costo de inventario y el riesgo de robo.

El año pasado, decidió examinar más de cerca sus cadenas de suministro existentes. Consciente de las entregas tardías o interrumpidas anteriores de suministros de cobre, la empresa decidió establecer acuerdos de compra con dos nuevos proveedores en América del Sur. Lo hizo de manera transparente, manteniendo a los dos proveedores con sede en Asia plenamente informados, para minimizar el impacto en sus operaciones. La empresa continuó haciendo negocios con ellos, aunque en volúmenes más bajos.

La aplicación de este tipo de enfoque avanzado y basado en el riesgo a sus cadenas de suministro demostró su valor poco después. Poco después de introducir el cambio, una gran tormenta destruyó una de las operaciones de los proveedores asiáticos, sin posibilidad de recuperación durante 12 meses debido a los grandes daños a su infraestructura física y de datos

LA BUENA EMPRESA – RESUMEN

- Retrasos ocasionales en el suministro de alambre de cobre de Asia, pero la empresa había afrontado estas interrupciones razonablemente bien. Hubo algunos impactos negativos en la satisfacción del cliente, pero estos se estaban gestionando.
- Estas interrupciones desencadenaron pensamientos sobre los daños mucho mayores que podrían ocurrir si un desastre mayor golpeara la zona donde se encontraban ambos proveedores de cobre. Se consideró que se trataba de un riesgo inaceptable de la cadena de suministro que representaría una seria amenaza para la sostenibilidad de la empresa.

Es evidente que la empresa había considerado el contexto, tanto el suyo como el de sus socios clave. Esto incluyó los objetivos de negocio relacionados con los costos de inventario de stock y el impacto potencial de las interrupciones en el flujo de efectivo, así como la satisfacción del cliente (en términos de calidad, capacidad de producción y entrega a tiempo).

Si bien estas circunstancias fueron descritas verbalmente por la dirección de la empresa, no tenían ninguna documentación formal, como un registro de emisiones o un registro de riesgos.

Sin embargo, parece que la empresa aplicó el RBT en términos de la probabilidad de perturbaciones perjudiciales para sus cadenas de suministro clave y el daño potencial que podrían causar, incluyendo impactos en su propia fiabilidad y sostenibilidad.

Podría decirse que la empresa había abordado este riesgo particular en términos de efecto e incertidumbre, basándose en un historial de problemas previamente conocidos y en el potencial de futuras interrupciones.

La ausencia de documentación formal no fue un problema en este caso porque se articuló suficiente evidencia verbal de la dirección. También había registros que demostraban sus acciones para mitigar el riesgo (por ejemplo, nuevos acuerdos con proveedores).

Este es un excelente ejemplo real de enfoque basado en el riesgo.

Estos dos estudios de caso ilustran lo que puede suceder en las organizaciones si el RBT no se aplica efectivamente como se requiere en la norma ISO 9001. También muestran cómo el RBT ayuda a las organizaciones a identificar y actuar sobre las oportunidades de mejora empresarial.

En este sentido, el RBT no es simplemente un enfoque para la gestión de riesgos; es una mentalidad positiva para el negocio que puede ofrecer beneficios empresariales significativos.

Conclusión

Mediante la identificación de riesgos clave, los impactos negativos a menudo se pueden evitar o minimizar. Las respuestas se pueden ajustar para ser más eficientes, eficaces y económicas.

El enfoque alternativo – no hacer nada hasta que se produce un fracaso, luego tener que implementar apresuradamente la corrección, la contención y las acciones correctivas– es generalmente más costoso y conlleva mayores riesgos para la marca, el negocio y la buena calidad. No es un enfoque viable.

Todas las organizaciones se enfrentaron a riesgos y oportunidades. El enfoque basado en el riesgo puede ayudarles a entender qué riesgos evitar y cuáles incorporar. Esto se traduce en un mejor cumplimiento, protege la marca y ayuda a alcanzar objetivos estratégicos.

En este sentido, el RBT no es simplemente un enfoque para la gestión de riesgos; es una mentalidad positiva para el negocio que puede ofrecer beneficios empresariales significativos.

Acerca de SAI Global

En SAI Global Assurance, entendemos los retos organizacionales de construir la confianza de las partes interesadas en todas las etapas de su proceso. Trabajamos con organizaciones para ayudarles a cumplir con las expectativas en cuanto a calidad, seguridad, sostenibilidad, integridad y conveniencia en cualquier mercado e industria a nivel mundial, al tiempo que incorporamos un pensamiento crítico basado en el riesgo y una cultura de mejora contínua.

SAI Global Assurance tiene oficinas en 21 países y ofrece servicios a clientes de todo el mundo, realizando más de 125.000 auditorías y formando a más de 100.000 estudiantes a través de sus cursos de aprendizaje.

Nuestros servicios incluyen:

- Auditoría e inspección - Una certificación acreditada con auditores expertos, respetados e independientes
- Aprendizaje y capacitación - Amplia gama de cursos acreditados para apoyar el avance profesional, el cambio de carrera o la mejora de la experiencia en la industria.
- Certificación de productos - Certificación de terceros contra normas conocidas para la conformidad de los productos.
- Asesoría Empresarial - Un equipo independiente para apoyar la mejora y el control del negocio, incluyendo sus cadenas de suministro.

Contacte con nosotros

Para más información, o para saber como SAI Global Assurance puede ayudar a su organización visite: **www.intertek.es/sai-global/**

intertek SAI GLOBAL