Galvanize
a Diligent brand

Hoja de soluciones

GESTIÓN DE RIESGO DE TERCEROS

Lista de verificación de la solución

A medida que las empresas subcontratan operaciones, se exponen a un mayor riesgo compartido con terceros. La mayoría de las organizaciones comprenden que necesitan automatizar las actividades de gestión de riesgos de terceros (TPRM, por sus siglas en inglés) para asegurarse de que gestionan y previenen los riesgos de manera eficaz. Pero muchas tienen dificultades para identificar y priorizar las características imprescindibles de una solución de TPRM. La siguiente lista de verificación de la solución resume las características claves que usted debe buscar.

FLUJO DE TRABAJO DE EVALUACIÓN DE RIESGOS DE TERCEROS

❑ Incorporación de terceros e inventario centralizado de terceros

Su solución debe contar con un repositorio centralizado de terceros y debe admitir:

+ Una función automatizada de importación en forma masiva para migrar terceros a la herramienta de TPRM.
+ Capacidad de integración con cuentas por pagar, etc.

❑ Planes de acciones correctivas

Una vez identificados las omisiones, usted debe ser capaz de seguir y automatizar la recomendación, aprobación y ejecución de los planes de acciones correctivas. La solución debe admitir la inclusión de usuarios de terceros en el flujo de trabajo del plan de acciones correctivas y permitirles crear planes, presentarlos para revisión y proporcionar actualizaciones del estado.

❑ Contenido listo para usar

Tanto si su entorno utiliza un control estandarizado de contenidos como HITRUST o Shared Assessments, o buenas prácticas de uso general como ISO, su solución debe ofrecer una biblioteca de contenidos que le permita instalarlos e implementarlos con prontitud.

❑ Flujos de trabajo de clasificación, evaluación y corrección listos para usar

Los procesos esenciales que necesita automatizar son:

+ Clasificación de terceros en categorías de alto nivel basadas en la criticidad.
+ Distribución y recolección de evaluaciones basadas en esas criticidades.
+ Identificación y corrección de omisiones basadas en las respuestas a esas evaluaciones.

Aunque el enfoque de TPRM de cada empresa es único, el suyo no es el primero que resuelve esos procesos esenciales. Su solución debe aprovechar las mejores prácticas de la industria para automatizar el proceso de evaluación.

PARTICIPACIÓN DE TERCEROS

❑ Asignación de cuestionarios de control basada en la criticidad

Muchas organizaciones cometen el error de hacer las mismas preguntas a cada uno de los terceros, recopilar enormes cantidades de datos e intentar descifrarlos. En consecuencia, suelen tener dificultades para obtener respuestas valiosas de los terceros y ahogan a su personal en un papeleo innecesario.

Se necesitan cuestionarios breves de clasificación para identificar rápidamente los riesgos de alto nivel y los niveles de criticidad de las relaciones con terceros, y cuestionarios específicos para preguntar solo lo que es necesario saber.

REQUISITOS DE LOS REPORTES DE RIESGOS

❑ Tableros de mando y reportes

Su solución de TPRM debe venir con una amplia biblioteca lista para usar, tableros de mando basados en roles y reportes con una variedad de estilos de presentación (p. ej., reportes de detalles de terceros, reportes de listas, gráficos y tablas). También debe asegurarse de que la herramienta le permita crear, modificar y publicar tableros de mando.

❑ Categorización y calificación flexibles de los riesgos

Su solución debe proporcionar informes valiosos que muestren los riesgos de terceros en todas las áreas importantes. Una cosa que aprendimos después de tantas implementaciones en tantas organizaciones diferentes es que cada una sigue sus propias y exclusivas categorías, prioridades y tolerancias de riesgos. Asegúrese de que su sistema sea suficientemente flexible para adaptarse a lo que para usted es exclusivo y que pueda crecer con los perfiles de riesgos cambiantes de su organización.

❑ Registro de documentos

Su solución de TPRM debe ofrecer la capacidad de seguir los adjuntos de los documentos como parte del perfil de un tercero. Los adjuntos pueden incluir elementos como estados financieros, documentos de incorporación, políticas y procedimientos, revisión de cumplimiento y reportes de diligencia debida.

❑ Monitoreo continuo

La gestión de riesgo de terceros es un proceso continuo. El monitoreo continuo puede lograrse de diversas formas; algunas de las comunes son:

+ Automatizar la programación de las evaluaciones de seguimiento sobre la base del nivel de riesgo de un tercero. La evaluación de un tercero de bajo riesgo se puede programar para que se repita cada tres años, mientras que un tercero crítico puede requerir revisiones trimestrales.
+ Integrar fuentes de inteligencia de terceros que proporcionen alertas de monitoreo continuo ante cambios significativos de la calificación de riesgo de un tercero (p. ej., calificación crediticia, calificación de riesgos de seguridad informática, nuevas apariciones en medios adversos o en listas de vigilancia del gobierno).

ARQUITECTURA E INFRAESTRUCTURA

❑ Flexibilidad para adaptarse a la evolución de los requisitos

Los requisitos normativos, las expectativas de las partes interesadas, las metas estratégicas y los riesgos identificados por su organización seguirán cambiando a lo largo del tiempo. Lo último que necesita es una solución rígida de TPRM que no le permita seguir el ritmo. Busque soluciones que puedan adaptarse rápidamente a los cambios de contenido de los cuestionarios, captura de metadatos, metodologías de calificación y priorización, flujos de trabajo e integraciones con otros sistemas.

❑ Integración con otros sistemas e inteligencia de terceros

Su solución de TPRM debe tener la capacidad de integrarse con los sistemas internos como LDAP, compras y cuentas por pagar, y con contenidos de inteligencia de terceros. Entre los ejemplos se encuentran las fuentes que pueden aumentar sus evaluaciones internas con información objetiva sobre la postura de seguridad informática de un tercero, su viabilidad financiera o su postura de cumplimiento.

OBTENGA MÁS INFORMACIÓN
wegalvanize.com/vendor-risk-management

POR QUÉ ELEGIR GALVANIZE

Galvanize, a Diligent Brand, es el principal proveedor de software de GRC para profesionales de seguridad, gestión de riesgos, cumplimiento y auditoría. La plataforma integrada HighBond aporta visibilidad sobre los riesgos, facilita la demostración del cumplimiento y ayuda a incrementar los programas de auditoría, riesgo y cumplimiento sin incurrir en costos adicionales.

Conozca más acerca de lo que puede lograr con Galvanize
1 604 646 4254 | wegalvanize.com | info@wegalvanize.com