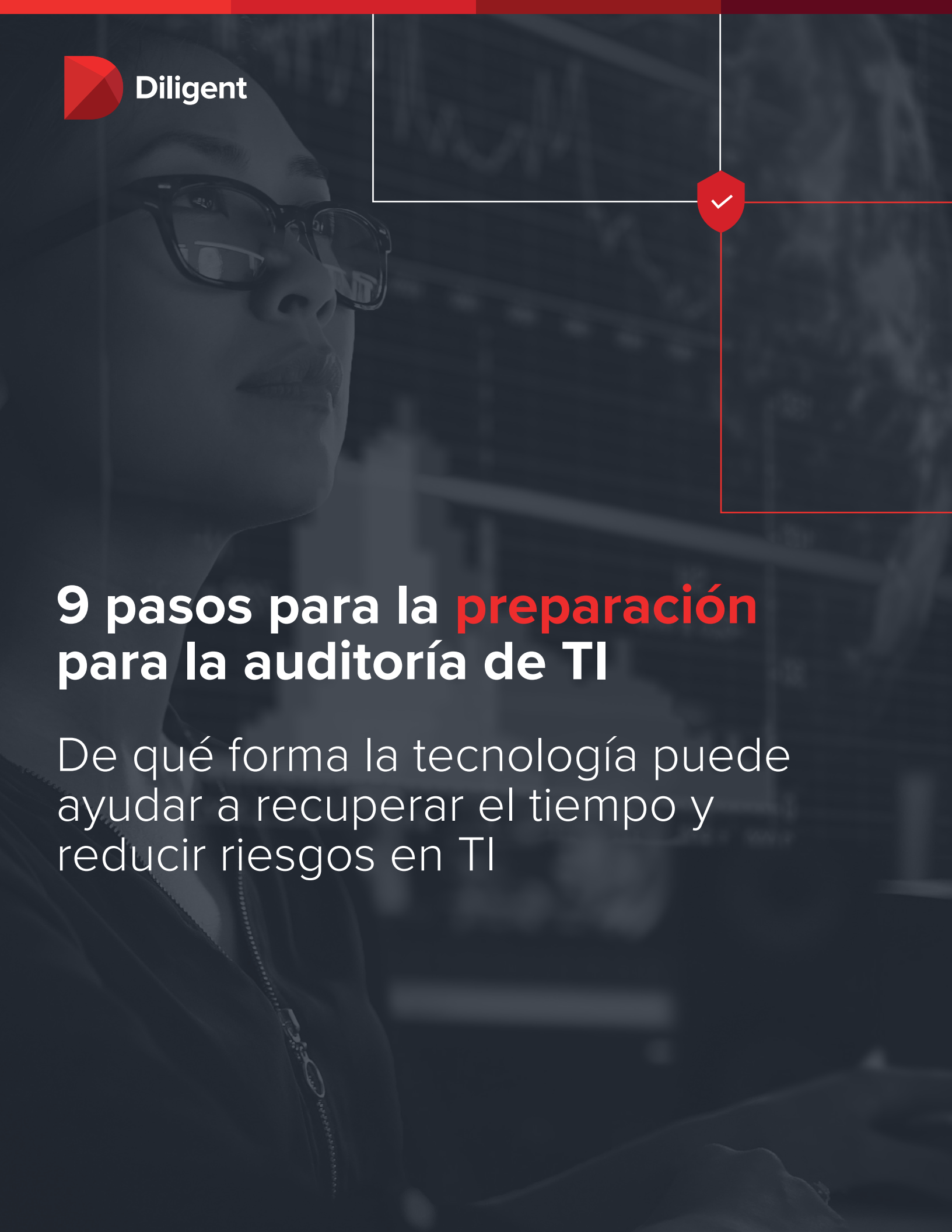

Diligent

9 pasos para la preparación para la auditoría de TI

De qué forma la tecnología puede ayudar a recuperar el tiempo y reducir riesgos en TI

Contenido

Su guía a la preparación de la auditoría de TI

Los riesgos de TI global y el marco normativo son cada vez más complejos. Y, para confundir más las cosas, existen cada vez más dispositivos, sistemas y datos, que crean aún más riesgos.

Detallamos nueve pasos clave para que la gestión de riesgo y las actividades de cumplimiento sean más inteligentes, veloces y hagan un uso menos intensivo de los recursos. Siga los pasos y podrá gestionar mejor los riesgos de TI, reducir la complejidad y los problemas de la gestión de TI y brindar mejores ideas a la gestión.

NUNCA ANTES LOS GERENTES DE TI ENFRENTARON TANTOS DESAFÍOS COMO HOY EN DÍA

Según el sector industrial y la región, existe una cantidad de marcos y regulaciones de cumplimiento con los que debe lidiar (p. ej., Ley Sarbanes-Oxley [SOX], Oficina de Administración y Presupuesto [OMB] A-123, Industria de tarjetas de pago [PCI], Ley Gramm–Leach–Bliley [GLBA], Ley de Portabilidad y Responsabilidad del Seguro de Salud [HIPAA], Objetivos de control para la información y tecnologías relacionadas [COBIT], Comité de Organizaciones Patrocinadoras de la Comisión Treadway [COSO], Organización Internacional de Normalización [ISO] y Declaraciones sobre normas para los compromisos de atestiguamiento [SSAE] 16 Controles de organizaciones de servicio [SOC] 1). Los auditores y especialistas en cumplimiento, tanto internos como externos, recurren al departamento de TI para identificar problemas de control.

Por eso, se genera una gran cantidad de trabajo para los recursos generalmente limitados del equipo de TI. Sin embargo, existe un riesgo verdadero de que una violación de la seguridad de datos o una falla grave en el sistema de TI genere daños importantes en la organización.

Dadas todas estas responsabilidades, lograr un estado de preparación para la auditoría de TI podría parecer una utopía. Pero se pueden llevar a cabo procesos para realizar evaluaciones de riesgo actualizadas y significativas y controles administrados y bien documentados, y para minimizar los resultados negativos en las auditorías. El problema es que organizarse para que las auditorías no sean un evento temido puede ser difícil.

Como en muchas funciones comerciales, implementar la tecnología adecuada puede ser la diferencia entre el éxito y el fracaso. Algunas organizaciones intentan administrar los procesos de cumplimiento, controles y riesgos de TI con tecnologías y herramientas genéricas, o que simplemente no se hicieron para esa función. Es mucho más probable que transforme la manera en la que se administran los procesos de cumplimiento y controles de TI si implementa tecnologías que estén creadas con esos objetivos. A medida que recorra estos nueve pasos, también verá que incluimos una lista de verificación de tecnología en casa paso, para que se asegure de tener las herramientas apropiadas para el trabajo.

Diligent

¿Por qué TI debe prepararse para una auditoría?

Las organizaciones confían en los procesos y sistemas de TI para mantener la competitividad y cumplir con sus misiones. La preparación para una auditoría ayuda a TI a recuperar el tiempo asignado a tareas esenciales y mejorar la administración de riesgos.

Si bien la gran cantidad de requisitos normativos y de cumplimiento interno puede parecer un ejercicio burocrático y de reglamentación, existe por un motivo. Los requisitos normativos y de cumplimiento interno protegen a la organización, la ayudan a alcanzar sus objetivos y la protegen del público y de terceros.

Esto es muy relevante para TI, ya que la mayoría de los negocios ahora dependen por completo de los procesos y sistemas de TI. Si algo sale mal, las consecuencias pueden ser desastrosas, como se vio cuando ocurrieron violaciones en la seguridad de datos de empresas como Target y Sony.

El objetivo de las iniciativas de preparación para la auditoría de TI es mejorar el funcionamiento. Prepararse para una auditoría de TI significa que los controles, incluidos los controles relacionados con TI, se vuelvan más efectivos, y los reportes financieros sean más precisos y confiables.

Como gerente de TI, debe administrar los riesgos de TI, llevar adelante de forma eficiente una auditoría de seguridad, control y cumplimiento de TI, y evitar sorpresas en un reporte de auditoría.

Si está preparado y puede dedicar menos tiempo a las auditorías, tendrá más tiempo disponible para el trabajo necesario para la misión en actualizaciones de sistemas comerciales y de infraestructura.

REÚNA AL EQUIPO

Los procesos y la tecnología son dos partes clave de la ecuación. El tercer componente son las personas. Ninguna iniciativa de preparación para una auditoría puede tener éxito si las personas no entienden por qué lo están haciendo, o si no están preparadas para involucrarse con los objetivos y las actividades.

Suele ser útil comenzar formando un equipo multifuncional o interdisciplinario que ayude a diseñar e impulsar el proceso. Como TI se conecta e interactúa con tantas áreas diferentes de la organización, esto seguramente implique reunir la experiencia de representantes de áreas funcionales, como los controles financieros, operaciones, auditoría interna y roles dentro del equipo mismo de TI (p. ej., especialistas en datos y seguridad).

Por último, asegúrese de tener soporte de liderazgo para los objetivos de preparación de la auditoría y alguien que pueda ayudarlo a superar obstáculos que puedan surgir.

Ya está listo para comenzar.

9 pasos para la preparación para la auditoría de TI

Una vez resueltos los temas introductorios, ocupémonos de los pasos que debe seguir para asegurarse de estar preparado para una auditoría.

01
Identificar y evaluar los riesgos de TI

Comience con los riesgos que tienen más impacto estratégico, incluidos los riesgos emergentes, normativos y operativos. Este es el paso principal de cualquier proceso de administración de riesgos.

Para identificar y crear el universo de riesgos, primero clasifique los riesgos por impacto. Algunos ejemplos:

01 **Impacto importante:** Las fallas en ciberseguridad llevan al robo de bases de datos de clientes; falla en la implementación de nuevos sistemas ERP

02 **Impacto medio:** Multas por incumplimiento del Reglamento General de Protección de Datos

03 **Impacto bajo:** Fraude por parte de un empleado por el uso de una identificación con acceso de superusuario

A continuación, asocie los riesgos al potencial impacto que podrían tener para lograr los objetivos estratégicos generales de la organización. Recuerde que los riesgos siempre deben ser:

- Cuantificados en cuanto a posible impacto financiero o de otro tipo
- Evaluados en términos de probabilidad
- Clasificados en relación con otros riesgos

Riesgos nuevos y emergentes

La administración de riesgos debe ser un proceso continuo que se lleve a cabo durante el año, ya que depende de la existencia y efectividad de los controles que se realicen para mitigar los riesgos.

Este paso también incluye un proceso continuo de identificación de riesgos nuevos y emergentes. Esto significa estar siempre al tanto del conjunto de normas y requisitos de cumplimiento de TI en cambio constante.

Este proceso requiere una mezcla de conocimiento y habilidades de pensamiento crítico, y, cuando convenga, análisis de datos para ayudarlo a monitorear las tendencias de riesgo cambiantes y valores atípicos. Los ejemplos típicos de conjuntos de datos que indican posibles riesgos de TI incluyen registros de acceso a bases de datos y redes, tablas de autorización y registros de transferencia de archivos.

DESAFÍOS EN ESTA ETAPA

- Confiar en que su variedad de riesgos y requisitos normativos son lo suficientemente exhaustivos
- Normalizar y evaluar los riesgos identificados en distintas áreas que usan tecnologías y métodos en conflicto
- Mantenerse al tanto del conjunto actual de requisitos normativos y de cumplimiento de TI
- Obtener información sobre nuevos riesgos posibles sin tecnología de análisis

REQUISITOS TECNOLÓGICOS

- Clasificar y reportar riesgos según distintos criterios
- Comparar riesgos estratégicos en relación a otros riesgos
- Asociar riesgos a objetivos estratégicos y las entidades en las que impactan
- Asociar riesgos a los requisitos normativos y de cumplimiento relevantes
- Asociar riesgos a los marcos normativos y de cumplimiento, riesgo o TI
- Registrar descripciones, categorías, clasificaciones de la evaluación, cuantificación y probabilidad de los riesgos
- Acceder a una gran variedad de archivos de datos del sistema y analizarlos
- Generar estadísticas e indicaciones de anomalías y valores atípicos
- Proporcionar análisis visual para ayudar a indicar tendencias y factores de los riesgos

Diligent

02
Identificar los controles

Los riesgos identificados en el primer paso ahora se deben coordinar con los controles que prevengan o reduzcan las posibilidades de que esos riesgos ocurran.

No a todos los riesgos les corresponderá un control necesariamente. Es posible que deba aceptar el riesgo de que ocurra un evento negativo, generalmente si se espera que el costo de un control eficiente sea mayor que la posible pérdida.

Durante este proceso, debería considerar la tolerancia al riesgo empresarial que determine la alta gerencia.

EJEMPLOS DE CONTROLES

- Firewalls para evitar acceso externo a los sistemas
- Tablas de autorización y acceso para restringir a usuarios
- Metodologías para reducir la probabilidad de fallas en los proyectos de desarrollo de sistemas nuevos

En esta etapa, los procedimientos de control y reducción de riesgos están definidos y documentados. Se puede tener en cuenta la estimación de los costos de implementación y mantenimiento de un control. La descripción y documentación de controles debe tener el detalle suficiente para admitir una revisión y auditoría independiente.

DESAFÍOS EN ESTA ETAPA

- Al igual que en el primer paso, puede resultar difícil encontrar y revisar todos los controles de mitigación entre una gran variedad de fuentes en toda la organización

REQUISITOS TECNOLÓGICOS

- Registre los controles en un marco reutilizable y administrado centralmente con el detalle suficiente para admitir procesos de revisión y auditoría (p. ej., respaldado con texto, gráficos y diagramas de flujo)
- Asigne los controles a los riesgos (tanto estratégicos como micro)
- Permita una administración de cambios sencilla para actualizar los controles de manera centralizada y derive los cambios a plantillas de proyecto de TI, así como a los auditores internos o externos que realicen revisiones

03
Asignar los controles a una biblioteca maestra

Mejore la supervisión de sus controles de riesgo de TI.

El proceso de identificar los controles de mitigación está conectado con el proceso de asignarlos, cuando sea posible, a una biblioteca general de marco de control. De esta forma, se estructuran las relaciones entre los controles, los propietarios de los controles y los requisitos normativos.

Los marcos de control de terceros se mantienen de forma independiente y se actualizan para reflejar los requisitos normativos nuevos y cambiantes, así como las mejores prácticas.

DESAFÍOS EN ESTA ETAPA

- Confiar en que su variedad de riesgos y requisitos normativos son lo suficientemente exhaustivos
- Normalizar y evaluar los riesgos identificados en distintas áreas que usan tecnologías y métodos en conflicto
- Mantenerse al tanto del conjunto actual de las normas y requisitos de cumplimiento de TI
- Obtener información sobre nuevos riesgos posibles sin tecnología de análisis

REQUISITOS TECNOLÓGICOS

- Clasificar y reportar riesgos según distintos criterios
- Comparar riesgos estratégicos en relación a otros riesgos
- Asociar riesgos a los objetivos estratégicos
- Asociar a los requisitos normativos y de cumplimiento relevantes
- Asociar a los marcos normativos y de cumplimiento, riesgo o TI
- Registrar descripciones, categorías, clasificación de evaluación, cuantificación y probabilidad de los riesgos
- Acceder a una gran variedad de archivos de datos y analizarlos
- Generar estadísticas e indicaciones de anomalías
- Proporcionar análisis visual para ayudar a indicar tendencias y factores de los riesgos

Diligent

04
Planificar, definir el alcance y realizar pruebas de estrés de los microrriesgos

¿Cuánto riesgo es aceptable?

Los controles están diseñados para combatir riesgos en distintos niveles y puede aumentar su nivel de detalle (micro) para reflejar vulnerabilidades y posibilidades específicas. Una parte de realizar una administración de riesgos eficiente es saber cuándo es razonable aceptar un riesgo particular y hasta dónde llegar en la implementación de un control.

En algún momento, es posible que los costos de la reducción de riesgos sobrepasen la magnitud de los daños posibles. Sin embargo, para administrar esto con eficiencia, debe evaluar consistentemente la magnitud de los riesgos en relación a los controles diseñados. También significa poder comunicar a la alta gerencia el impacto general de los riesgos aceptados y fallas de control.

DESAFÍOS EN ESTA ETAPA

- Cuantificar el aseguramiento de los riesgos que TI proporciona a la organización
- Tomar las medidas adecuadas si un microrriesgo se evalúa como de alto impacto y de alta probabilidad
- Comprender el riesgo que corre la organización si falla un control
- Consolidar y reportar los esfuerzos generales de riesgo y control es difícil
- Asegurar que los datos sean consistentes y estén organizados

REQUISITOS TECNOLÓGICOS

- Evaluar y sopesar la efectividad de los controles de TI diseñados para mitigar riesgos a nivel micro
- Recopilar, fusionar y normalizar datos de varias fuentes
- Cuantificar el aseguramiento de riesgos según el control, el objetivo del control y el proyecto de TI

Diligent

05
Evaluar la eficacia de los controles

Una parte importante de la preparación para una auditoría es asegurarse de que los controles realmente funcionen como deberían. El análisis de datos es clave cuando se trata de evaluar la eficiencia de los controles, de modo que puede consultar y examinar los conjuntos de datos completos para ver qué sucedió durante un período determinado.

Los controles también pueden pasar por una autoevaluación por parte de sus propietarios mediante cuestionarios periódicos. En algunos casos, las actividades de los propietarios de controles pueden formar parte del proceso de certificación que contribuye a la aprobación, por parte de la alta gerencia, de la implementación de sistemas de control eficientes.

Las evaluaciones de controles suelen realizarse periódicamente. Sin embargo, deberían considerarse junto con el sexto paso, en el que los controles clave se monitorean mediante técnicas automatizadas continuas.

DESAFÍOS EN ESTA ETAPA

- Determinar si los controles funcionan realmente o no
- Determinar si sus controles se están ignorando o eludiendo
- Realizar un seguimiento de quiénes son responsables de qué controles y asegurarse de que no se distraigan

REQUISITOS TECNOLÓGICOS

- Automatizar y analizar encuestas y cuestionarios
- Visualizar los datos acumulados de varias pruebas para dar sentido a los valores atípicos
- Realizar pruebas sobre una gran variedad de tipos de fracasos de los controles

06
Capturar, seguir y reportar las deficiencias

Mientras más rápido identifique las debilidades de los controles, más rápido podrán abordarse y resolverse.

Cuando se identifican las deficiencias en los controles, es importante responder rápidamente para reparar y mejorar el proceso de control. En muchos casos, los análisis de datos recurrentes pueden usarse para fortalecer los controles o crear un nivel de control adicional.

Por ejemplo, si los controles de acceso a datos confidenciales parecieran no ser del todo eficientes, se pueden realizar análisis de datos regularmente para identificar instancias de acceso riesgoso. Al identificarlas temprano, se pueden abordar antes de que generen problemas más grandes.

DESAFÍOS EN ESTA ETAPA

- Hacer controles realmente eficientes
- Resistencia de quienes quieren terminar rápido el trabajo y eludir los controles

REQUISITOS TECNOLÓGICOS

- Capacidad de realizar un seguimiento centralizado de las respuestas a las deficiencias de controles identificadas
- Identificar transacciones riesgosas según una amplia gama de criterios de prueba

Diligent

07
Monitorear y automatizar las pruebas de los controles

Implementar software especializado le permite automatizar las pruebas de controles, aumentar la eficiencia y devolverle el tiempo valioso de pensamiento crítico al personal de TI.

Todos los pasos del proceso de preparación de la auditoría son importantes, pero el monitoreo agrega un componente esencial, que brinda una evaluación actualizada de la efectividad de las actividades de control y gestión de riesgos de TI. Además, puede ayudarlo a identificar indicadores de riesgos nuevos para los cuales no haya controles.

En casi todos los casos, el análisis de datos es efectivo para probar controles y evaluar riesgos. Considere ejecutar formas similares de análisis de datos de manera continua, es decir, diaria, semanal o mensualmente, lo que mejor sirva para su organización.

EL MONITOREO DE ESTUDIOS ANALÍTICOS PUEDE APLICARSE A MUCHAS ACTIVIDADES DE TI

- Uso de acceso especial y de administrador a sistemas
- División de tareas
- Cambios o anulaciones de controles
- Cambios en el firewall
- Cambios en los datos cruciales
- Registros de red
- Registros de acceso físico

DESAFÍOS EN ESTA ETAPA

- El enfoque tradicional al monitoreo de la efectividad de los controles incluye métodos manuales, como revisar documentación o realizar revisiones de confiabilidad en los procedimientos de control
- Las pruebas manuales en un momento determinado no proporcionan aseguramiento o información sobre si los controles funcionaron de forma eficiente en todas las actividades durante determinado período

REQUISITOS TECNOLÓGICOS

- Capacidad de probar transacciones con regularidad (financieras, operativas y específicas de TI) con respecto a grandes conjuntos de datos
- Procedimientos de análisis y automatización de datos cuyos requisitos de recursos sean mínimos

08
Señalar las excepciones, revisar y corregir

Los pasos previos de monitoreo develan indicadores de potenciales problemas, que señalan que un control no funciona eficientemente o que determinado riesgo está aumentando.

Estas señales de alerta deben ser investigadas y resueltas por individuos que estén familiarizados con los procesos subyacentes y los controles que se deben ejecutar.

Durante este proceso (generalmente, llamado gestión de excepciones o gestión de asuntos), ten en cuenta que algunas señales de alerta serán falsos positivos, mientras otras podrían indicar fracasos reales en los controles.

Las acciones podrían incluir abordar el problema que ocurrió (p. ej., lidiar con el acceso no autorizado de un empleado a datos sensibles) o reparar el control para reducir las posibilidades de que vuelva a ocurrir.

Muchos falsos positivos pueden eliminarse ajustando la configuración de los análisis y las pruebas, de modo que los elementos no riesgosos no se reporten.

DESAFÍOS EN ESTA ETAPA

- La gestión de asuntos puede ser abrumadora, especialmente al abordar la enorme variedad de normas y requisitos de cumplimiento de TI
- Grandes volúmenes de falsos positivos pueden generar que se pasen por alto indicadores cuando hay un problema real con los controles
- Grandes volúmenes de excepciones que se generen en varios sistemas pueden resultar en un uso intensivo de los recursos y ser difíciles de administrar
- Si se identifican debilidades en los controles y transacciones riesgosas, pero no se abordan, la administración no sabrá cuál es la magnitud de los problemas

REQUISITOS TECNOLÓGICOS

- Ajustar los procedimientos de prueba de modo que las actividades sin riesgo o de bajo riesgo no se reporten como excepciones
- Establecer y modificar procedimientos del flujo de trabajo con facilidad
- Escalar automáticamente excepciones y transacciones riesgosas a la alta gerencia para su revisión
- Informar el estado de las actividades de gestión de excepciones
- Informar del alcance del riesgo existente según los resultados de la investigación de excepciones

Diligent

09
Mejora continua

Si refina los controles y procesos de monitoreo (y usa tecnología especializada), se asegurará de estar preparado para una auditoría.

Con el tiempo, los riesgos se reducen y el proceso de control completo mejora mediante un ciclo continuo de pruebas, monitoreo de controles y abordaje de asuntos excepcionales.

Este proceso reduce notablemente la probabilidad de obtener resultados adversos en una auditoría. Ahora, cuando se investigue a TI mediante funciones de cumplimiento y auditorías (internas o externas), no habrá sorpresas.

DESAFÍOS EN ESTA ETAPA

- Puede resultar difícil gestionar todas las partes en movimiento y mantenerse concentrado en los riesgos más significativos y controles más importantes
- Usar métodos manuales o una gran variedad de sistemas caseros, generalmente en hojas de cálculo, consume mucho tiempo y no suele ser efectivo

REQUISITOS TECNOLÓGICOS

- Soporte para todas las etapas del proceso de monitoreo y evaluación de controles o riesgos
- Crear reportes que proporcionen información sobre el estado general de la preparación para una auditoría en toda la infraestructura de TI

¡Felicitaciones! Después de seguir los 9 pasos, llegó al tan codiciado estado de preparación para una auditoría.

PASO EXTRA

Tendencia predictiva del riesgo de TI

Alcanzó la preparación para una auditoría, ahora es momento de ir un paso más allá. Asegúrese de que los sistemas de control de TI funcionen correctamente, y comience a informar los resultados de todo el proceso.

Si usas tableros de mando y mapas de riesgo, puedes brindar pruebas visuales y cuantificables de los procedimientos de prueba y análisis realizados, junto con los resultados. Estos reportes de alto nivel muestran tendencias a lo largo del tiempo para asuntos de control o riesgo, categorizados según criterios, como región, función comercial o gerente. Además, podrás encontrar las áreas en las que es más probable que se desarrollen problemas más serios.

DESAFÍOS EN ESTA ETAPA

- Resulta muy laborioso recopilar información de varias fuentes de toda la organización y presentarla de forma que tenga sentido tanto a nivel técnico como para la alta gerencia
- Proporcionar contexto para los asuntos de control y riesgo, y la naturaleza y el alcance de las actividades de prueba y monitoreo, sin tecnología especializada es difícil

REQUISITOS TECNOLÓGICOS

- Acumular datos sobre la naturaleza y el volumen de las actividades de prueba, los resultados y las respuestas de seguimiento
- Realizar reportes exhaustivos sobre el estado de las actividades realizadas, incluidos el alcance cuantificado de las pruebas, los resultados y las respuestas
- Asociar los datos de las pruebas y respuestas con los controles y riesgos subyacentes

Diligent

PASO EXTRA

Integrar la gestión de riesgos de TI a la gestión de riesgos empresariales (GRE) general

A veces, el objetivo principal de lograr la preparación para una auditoría de TI es gestionar mejor las responsabilidades de cumplimiento y control de los departamentos. En otros casos, es útil mirar los procesos de TI de gestión de riesgos, control y cumplimiento en un contexto más amplio de actividades de gestión de riesgos empresariales (GRE).

Al tomar un enfoque más amplio, la alta gerencia corporativa u organizativa puede mirar los riesgos de TI junto a esas categorías de riesgos y áreas funcionales clave para obtener una imagen más completa.

Otro beneficio de tomar un enfoque más integrado es que resulta más fácil mostrar cómo se interrelacionan los riesgos y controles. Los riesgos de TI no suelen darse de forma aislada, sino que, generalmente, deben considerarse los riesgos y controles en conjunto dentro de sistemas financieros y operativos específicos.

DESAFÍOS EN ESTA ETAPA

- Distintas entidades involucradas en el control y la gestión de riesgos dentro de una organización podrían evaluar riesgos y controlar asuntos de distintas formas, lo que dificulta que la gerencia reciba una imagen comparativa comprensible
- Las organizaciones podrían usar una variedad de tecnologías y enfoques para la evaluación de riesgos y el control de asuntos y la preparación para auditorías en diferentes áreas
- Crear una vista exhaustiva de la preparación para auditorías en varias áreas funcionales no es fácil

REQUISITOS TECNOLÓGICOS

- Abordar una amplia variedad de actividades de auditoría y riesgo y control en distintas áreas organizativas
- Integrar con otras tecnologías de gestión de riesgos y control

Diligent

Preparación de la auditoría de TI: Ganamos todos

Por eso, vale la pena hacerlo bien y utilizar la tecnología apropiada.

Estos nueve pasos lo ayudarán a transformar lo que suele ser un proceso arduo, frustrante e ineficiente en uno que requiera mucho menos esfuerzo y que reduzca significativamente los costos generales de recursos.

Hay muchas tecnologías disponibles para brindar soporte al proceso de seguridad y control de TI. Sin embargo, uno de los mayores desafíos es gestionar el proceso completo de forma consistente para obtener una vista exhaustiva del estado de los riesgos y el cumplimiento de TI en un solo lugar.

La plataforma de Gestión de auditoría de TI de Diligent integra su marco de riesgos de TI para brindarle la estructura que necesita para asegurarse de que el entorno de seguridad de TI sea robusto, esté bien administrado y alineado con riesgos estratégicos.

BENEFICIOS CLAVE

- La preparación para una auditoría beneficia a la función de TI, así como la organización general
- Sabe que los riesgos de TI están realmente bien administrados
- Los reguladores y auditores están más conformes y tienen menos asuntos negativos que informar
- La gestión de TI mejora la información y el aseguramiento proporcionados a la alta gerencia
- La probabilidad de que un asunto de control o cumplimiento cause daños significativos a la organización se reduce notablemente

¿Está listo para aprender cómo nuestra plataforma de Gestión de auditoría puede ayudarlo a estar preparado para las auditorías?

Acerca del autor

John Verver, CPA CA, CMC, CISA (contador público colegiado, consultor certificado, auditor de sistemas de información)

John Verver es el antiguo vicepresidente de Diligent. Dentro de sus responsabilidades estaban la estrategia de productos y servicios, así como el liderazgo y el crecimiento de los servicios profesionales.

Como experto y líder de opinión sobre el uso de tecnología (en particular, los estudios analíticos y la automatización de los datos) para la gobernanza empresarial, John es un orador habitual en las conferencias mundiales y colabora frecuentemente con artículos en las publicaciones profesionales y de negocios.

Acerca de Diligent Corporation

Diligent es el principal proveedor de servicios de software (SaaS) de gobernanza, riesgo y cumplimiento (GRC) y atiende a más de un millón de usuarios de más de 25 000 organizaciones alrededor del mundo. Nuestra moderna plataforma de GRC asegura que las juntas directivas, los ejecutivos y otros líderes tengan una visión holística e integrada de auditoría, riesgo, seguridad de la información, ética y cumplimiento en toda la organización. Diligent brinda tecnología, información y confianza a los líderes para que puedan crear organizaciones más eficaces, equitativas y exitosas.

Para obtener más información o solicitar una demostración:

Correo electrónico: info@diligent.com | Visite: diligent.com