Diligent

Tener controles frente a tener el control

La evolución del rol de CCO y la puesta en práctica de un marco de control efectivo

Contenido

La gestión de riesgos es un deporte de equipo

Una gestión de riesgos eficaz en una institución financiera no se reduce a un único equipo o interesado.

Es una iniciativa que abarca toda la empresa y depende de un sistema integral de gobernanza. Y va mucho más allá del monitoreo de los riesgos financieros. Las empresas necesitan controlar los riesgos que conllevan factores como las violaciones de la ciberseguridad, el riesgo de proveedores externos, los fraudes financieros, las fallas de la cadena de suministros y otras formas de riesgos operacionales.


Diligent

Las tres líneas de defensa

Muchas instituciones cuentan con un modelo de tres capas, comúnmente conocido como sistema de Tres Líneas de Defensa (3LOD, por sus siglas en inglés), para controlar, gestionar y auditar los riesgos.

Esto incluye tres roles o equipos independientes:

01 **La primera línea:** funciones responsables de la gestión de riesgos

02 **La segunda línea:** funciones que supervisan el riesgo

03 **La tercera línea:** funciones que proporcionan auditorías independientes

En la primera línea de defensa, la gerencia operativa, que suele incluir un director de controles (CCO, por sus siglas en inglés) y un equipo de gerentes, define la visión y el marco para las políticas de gestión de riesgos de la empresa e implementa y supervisa los controles que mitigarán los riesgos. La segunda línea cuenta con varias funciones, que incluyen gestión de riesgos, cumplimiento y contraloría; todas funcionando juntas para asegurar que se sigan los controles y se identifiquen diariamente los cambios de las variables de riesgo. La tercera línea tiene la responsabilidad de asegurar la eficacia de las otras dos líneas con auditores independientes que revisan y analizan todos los aspectos de los marcos de control y gestión de riesgos, y proporcionan valoraciones a la directiva y las otras sucursales para apoyar los procesos de optimización.

Aunque las tres líneas son esenciales para el desarrollo de un proceso de gestión de riesgos altamente eficaz, para comenzar es necesario centrarse en la primera línea de defensa. Asegurar que su institución financiera creó y está gestionando un marco de control integral le permitirá mitigar una importante cantidad de riesgos con los procesos ya implementados. En este libro electrónico, analizaremos la evolución del rol de CCO y cómo poner en práctica un marco de controles efectivos.

La evolución del CCO

A pesar de que los bancos siempre tienen estrechamente controlados los datos financieros y el acceso, el rol de CCO se ha desarrollado en los años recientes debido a la necesidad de mayores restricciones y requisitos de cumplimiento en relación con las transacciones no financieras.

A medida que aumenta la prevalencia de las violaciones de ciberseguridad, los fraudes y los factores de riesgo de terceros, y los requisitos de cumplimiento se vuelven más exigentes, es importante que las instituciones financieras cuenten con un rol de liderazgo dedicado a crear políticas para mantener controles férreos sobre todos los factores de riesgo operacional y hacerlas cumplir.

AUMENTAN LAS MULTAS Y LA TASA DE LIQUIDACIÓN

Las organizaciones nunca han tenido tanto en juego: las que no cumplen con las normas del gobierno o de la industria pueden enfrentar enormes multas y un potencial encarcelamiento de sus empleados si existen delitos claros, además del daño a la reputación del que pueden demorar años en recuperarse. Un estudio de McKinsey del 2016 reveló que las multas y las tasas de liquidación se habían multiplicado casi por 45 desde 2009.[1] Además, como las organizaciones suelen tener sucursales distribuidas en todo el mundo (y ahora, debido a la pandemia de COVID-19, muchas organizaciones tienen un alto porcentaje de trabajadores remotos), es más difícil que nunca calibrar adecuadamente los niveles de cumplimiento y de riesgo de toda la empresa.

LOS CCO SE SIENTAN A LA MESA

En general, el CCO tendrá oportunidad de un amplio mandato y una posición importante entre los directivos; lo más común es que ella o él reporte directamente al director de operaciones. Sin embargo, el CCO o director de riesgos se ha convertido en un rol tan crítico que el siguiente paso de su trayectoria quizás sea Presidente, como hemos visto en Barclays, que recientemente promovió al director de riesgos C. S. Venkatakrishnan a copresidente.[2]

A MEDIDA QUE AUMENTA EL RIESGO, TAMBIÉN AUMENTA LA NECESIDAD DE UN SISTEMA EFICAZ

Es probable que estemos viendo un crecimiento del protagonismo de la primera línea de defensa (1LoD) porque está claro que sin una primera línea fuerte, las otras carecen de eficacia. Es esencial crear un sistema sólido y eficaz para establecer y monitorear controles de primera línea en toda la empresa, que ayudarán a mitigar el riesgo en todas las facetas.

La respuesta al aumento natural de los factores externos no es la ampliación del tamaño de la segunda línea de defensa dedicada a la gestión de riesgos. En cambio, es crucial implementar un sistema integral en la 1LoD para la implementación y el seguimiento de los controles, y usar herramientas automatizadas para identificar los disparadores de riesgos en tiempo real.

[1] www.mckinsey.com/business-functions/risk/our-insights/a-best-practice-model-for-bank-compliance
[2] www.bloomberg.com/news/articles/2020-09-30/barclays-promotes-risk-head-in-sweeping-changes-to-leadership

Diligent

Tome el control de los controles, cualquiera sea su complejidad

Entonces, como CCO o director de riesgos, ¿cuáles son los primeros pasos que debe dar para dominar la complejidad del panorama de controles?

Considere las siguientes como sus prioridades iniciales:

DEFINA UN MARCO DE CONTROL INTEGRAL MÍNIMO

Primero, fíjese en sus objetivos organizacionales generales y diseñe un sistema de controles que se ajuste. Si tiene 10.000 ubicaciones en el mundo, es posible que encuentre variaciones regionales en la forma de operar de sus ubicaciones; por eso, en lugar de preocuparse por pequeñeces, piense primero en los asuntos operacionales que realmente afectan la seguridad o el cumplimiento de sus sucursales y básese en ellos. El proceso incluirá:

- Identificar los requisitos normativos y de cumplimiento de su sector y determinar cómo deben influir en sus procesos operacionales
- Determinar el apetito de riesgo de su empresa; ¿qué nivel de riesgo está dispuesto a asumir para cada factor de riesgo en relación con el nivel de la inversión necesaria?
- Desarrollar un proceso de identificación de gestión de riesgos que incluya un inventario de riesgos, cuadros de mando de evaluación de riesgos y una metodología de medición de riesgos
- Establecer programas de capacitación y protocolos para abordar los asuntos de cumplimiento y gestión de riesgos en todos los departamentos
- Desarrollar una cadena interna de mando y selección de personal para las principales contrataciones

CREAR UN SISTEMA PARA AUTOMATIZACIÓN

Cuando haya desarrollado los controles y disparadores de riesgo necesarios en su proceso, es importante desarrollar la pila de tecnología adecuada para ayudar a gestionar y monitorear sus factores de riesgo. Céntrese en pasar de procesos manuales a automatizados, comience con iniciativas pequeñas antes de implementar procesos automatizados en toda la empresa. Su software debe permitir un uso intuitivo y ofrecer oportunidades de aportar datos en tiempo real para el análisis de riesgos.

ASOCIE EXPERIENCIA HUMANA CON APRENDIZAJE AUTOMÁTICO

Una vez que cuente con un sistema de automatización para ayudar al seguimiento de los controles, puede aprovechar al máximo un sistema que asocia el aprendizaje automático con el análisis especializado de expertos en la materia. Mediante la asociación de tecnología con analistas humanos para corroborar datos y profundizar en los potenciales problemas, puede estar seguro de que sus especialistas dedican su tiempo a los análisis estratégicos en los que son expertos, en lugar de realizar simples tareas repetitivas.

Las enormes cantidades de datos y su disponibilidad inmediata —junto a nuevas tecnologías, nuevos modelos de negocios y cadenas de valor— están transformando la forma en la que los bancos sirven a sus clientes, interactúan con terceros y funcionan internamente. El departamento de riesgo operacional debe mantenerse al día con este entorno dinámico, incluido el cambiante panorama de riesgos.

Diligent

Usar KCI para guiar su madurez

A medida que desarrolla sus marcos de controles, es importante identificar los indicadores claves de los controles (KCI) además de los factores claves de riesgo (KRF, por sus siglas en inglés).

En lugar de enfocarse en los riesgos en sí mismos, sus KCI se centran en los factores de control que se usan para mitigar los riesgos y ayudan a comprender si los controles de la organización funcionan con eficacia.

IDENTIFICACIÓN DE KCI

Para identificar en cuáles KCI centrarse, piense en su organización desde el punto de vista estratégico y qué es lo que necesita mayor protección: datos, infraestructura, seguridad de la red u otros factores. Analice los protocolos de cumplimiento existentes y determine cuáles son los puntos de referencia para el éxito de estas iniciativas. Realice una auditoría preliminar para asegurarse de no estar introduciendo demasiadas herramientas en el proceso y de no estar creando redundancias que dificulten el seguimiento de sus KCI.

Para determinar sus niveles de KCI, debe evaluar y clasificar el desempeño de sus KCI sobre la base de una serie de medidas de referencia para comprender qué tan integral es su sistema de controles. Cuando sea posible, cada KCI puede clasificarse individualmente sobre la base del desempeño en diferentes unidades de negocios.

Por ejemplo, pensemos en un control potencial: prueba del plan de recuperación de desastres. Para determinar el KCI para esta medida en cada departamento, debe considerar cuestiones como:

- ¿La unidad de negocios tiene un plan documentado de recuperación de desastres?
- ¿Con qué frecuencia se prueba el plan de recuperación de desastres?
- ¿Con qué velocidad pudo restaurar todos los servicios después de hacer una prueba?
- ¿Tiene una lista de las partes interesadas claves y sus roles en el plan de recuperación de desastres?

Si algunos departamentos están retrasados con respecto a otros en cuanto a integralidad y frecuencia, será importante conversar claramente con ellos sobre un plan de mitigación y, luego, volver a probar sus KCI en una fecha posterior para confirmar su progreso en relación con las medidas claves.

MONITOREO DE KCI

El monitoreo de sus KCI debería ser un proceso continuo, con automatización incorporada donde sea posible para simplificar la generación de reportes y la auditoría. Mida, monitoree y converse con las unidades de negocios para optimizar cada KCI a lo largo del tiempo.

Para agilizar el proceso, simplifique y amalgame el diseño, las pruebas y la generación de reportes de sus controles. Cuando cree un sistema integral de inventario y clasificación de los controles, hable con todos los propietarios de las diferentes unidades de negocios para comprender qué hacen, por qué lo hacen y cómo contribuye lo que hacen a los objetivos empresariales. Sea paciente: este proceso puede llevar meses o incluso años, según el tamaño de su organización, pero le aportará claridad sobre cuáles controles y KCI deben ser los factores claves de su proceso de reportes.

Diligent

Integración con las 2LoD y 3LoD

Con proceso de controles claro y exhaustivo en funcionamiento, los roles de gestión de riesgos y auditoría deberían estar bien integrados en su proceso general de gobernanza.

Asegúrese de establecer una nítida división de tareas (SoD) en las tres líneas de defensa entre gestión y monitoreo de controles; inventario, control y monitoreo de riesgos; y auditorías generales y aseguramiento de calidad.

La creación de un proceso integral de controles le permitirá hacerse cargo de la responsabilidad y la transparencia de toda la junta. Su organización puede realizar un seguimiento de los riesgos, agregarlos a un inventario con facilidad y vincularlos con controles, así sabrá en cuáles controles es más importante invertir para mitigar riesgos y recibir alertas en tiempo real, incluidos disparadores de riesgo cuando no se siguen los controles. Sus auditores independientes pueden revisar datos de referencia de las mejores prácticas y monitorear si cada protocolo se sigue en todos los departamentos para, luego, presentar reportes detallados a su equipo de directores junto con recomendaciones para las medidas correctivas.

A pesar de que es probable que cada línea de defensa trabaje con cierto grado de independencia, crear una 1LoD sólida brindará un apoyo fuerte a las otras dos líneas, con beneficios como:

MAYORES NIVELES DE ASEGURAMIENTO

Muchas organizaciones han tenido incidentes de seguridad de alto perfil por fallas de los controles y falta de comunicación entre los equipos. Por ejemplo, el año pasado, la empresa de cambio de divisas TravelEx sufrió un cibersecuestro de datos que mantuvo a la empresa fuera de línea durante casi un mes. Los hackers dijeron que habían vulnerado los datos de la empresa seis meses antes, y descargaron 5 GB de datos de la empresa. Con la implementación de controles más férreos y un proceso de gestión de riesgos, este ataque no habría pasado inadvertido.

INTERACCIONES AUTOMATIZADAS ENTRE LOS PROPIETARIOS Y LOS RESPONSABLES DE LOS CONTROLES

Mediante la automatización de la transmisión de datos claves, los responsables y los operadores de los controles pueden monitorear la eficacia de los controles de forma sencilla y eficiente, y recomendar mejoras en el proceso cuando se necesitan.

RECOPILACIÓN Y ANÁLISIS AUTOMATIZADOS DE LOS DATOS OPERATIVOS

Su organización podrá monitorear los datos operacionales y realizar un seguimiento de qué tan bien se siguen los controles y los costos asociados en términos de infraestructura y horas trabajadas.

MAYOR ASEGURAMIENTO SIN AMPLIAR EL EQUIPO DE AUDITORÍA

El uso de un sistema automatizado de controles como columna vertebral de su protocolo de gestión de riesgos le permitirá proporcionar gran parte del trabajo preparatorio preliminar a su equipo de auditoría. Así, su equipo podrá hacer trabajos más productivos sin necesidad de dedicar tiempo de inventariar controles y riesgos.

Conclusión

Las mejores instituciones financieras ya no miran únicamente el riesgo financiero. Están configurando procesos integrales para implementar controles y mitigar riesgos operacionales de todo tipo, con protocolos agregados para monitorear qué tan bien se siguen los controles en los distintos departamentos. En lugar de depender de auditorías poco frecuentes para el seguimiento del éxito de sus esfuerzos, aprovechan el aprendizaje automático para obtener análisis en tiempo real del grado de cumplimiento de cada división con los puntos de referencia del proceso de los controles.

Al asegurar que sus controles están optimizados y que los errores dentro de los departamentos se corrigen rápidamente, puede quitar presión a su equipo de gestión de riesgos y reducir la probabilidad de que su organización se vea afectada por riesgos significativos.

Como vimos en 2020, sucesos sorpresivos y de gran impacto como la pandemia de COVID-19 pueden sembrar el caos en los planes mejor delineados e introducir incertidumbre en nuestros procesos existentes. Sin embargo, al crear un riguroso proceso de gestión de riesgos en tres capas que comienza con un sistema integral de controles para monitorear el cumplimiento y prevenir la materialización de los factores de riesgo, su organización estará bien posicionada para hacer frente a la próxima crisis e identificar los riesgos antes de que afecten su empresa.

Junto con su división de gestión de riesgos y su equipo de auditoría, podrá crear un proceso optimizado y eficiente para comprender dónde invertir en mitigación de riesgos y qué procesos implementar para monitorear el cumplimiento, ayudar a la organización a aprovechar al máximo su presupuesto de gestión de riesgos y proteger la empresa de incumplimientos y otros riesgos operacionales.

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