Aproximación basada en el riesgo y cuestiones organizativas

Serie de kits de despliegue
Compliance

Kit 3. Plan de acción para la tercera semana

Marzo 2016

www.kpmgcumplimientolegal.es

Briefing

Una cuestión de riesgo

Alain Casanovas
Socio de KPMG Abogados
acasanovas@kpmg.es

Perfil en LinkedIn

Puesto que el término "*Compliance*" puede traducirse al español como "cumplimiento", hay quien considera que esta función está vinculada con el conocimiento de las obligaciones que son **impuestas coercitivamente**. No obstante, los textos modernos incluyen también aquellas asumidas **voluntariamente** -sin que vengan exigidas a través de la coerción del Estado-, evitando equiparar el significado de *Compliance* con la acepción tradicional de "cumplimiento".

Que *Compliance* guarde relación con el cumplimiento de las obligaciones, otorga a la disciplina un **sesgo jurídico evidente**. No obstante, el objetivo que tiene para el *Compliance* Officer ese conocimiento de las obligaciones no es otro que establecer mecanismos que faciliten su aplicación, evitando y detectando los riesgos derivados de su **incumplimiento**. Tal circunstancia conduce a aplicar metodología del control de riesgos al ámbito del *Compliance*, y que el perfil del *Compliance* Officer sea entonces híbrido, al conjungar conocimientos del ámbito jurídico con la sistemática de la gestión de riesgos.

En este Kit verás cómo se aplican principios y criterios de la **gestión de riesgos** al ámbito del *Compliance*. Y, como comprobarás, no se trata de un ejercicio teórico, sino con un carácter eminentemente práctico y de gran importancia para diseñar un buen modelo de *Compliance*. Si procedes del ámbito de la auditoría o el control interno, estarás familiarizado con la práctica totalidad de sugerencias contenidas en el Kit; sin embargo, si eres jurista, es posible que algunas ideas te resulten nuevas y precises prestar algo más de atención. En cualquier caso, este Kit te ayudará a progresar con facilidad en la definición y despliegue de un modelo de *Compliance* avanzado, siguiendo aproximaciones basadas en el riesgo.

Índice

Plan de acción para la tercera semana

Este Kit de despliegue te ayudará a cubrir algunos objetivos importantes en la implantación del modelo de *Compliance*, incluyendo sugerencias de utilidad y referencias a otros documentos de consulta.

Objetivos a cubrir durante la tercera semana

Identificar los bloques de *Compliance* o dominios que estarán dentro del perímetro de sus competencias de supervisión.

Definir la composición del órgano de *Compliance* conforme con lo anterior.

Familiarizarte con la metodología de evaluación de riesgos que se utilice en tu organización.

Desarrollar un *risk assessment* relativo a los bloques de *Compliance* o dominios identificados anteriormente.

Importancia de seguir una aproximación basada en el riesgo

En un universo teórico con recursos ilimitados, toda organización podría disponer de medios para prevenir y detectar cualquier tipo de riesgos, por insignificantes que fuesen sus **probabilidades** de ocurrencia e **impacto**. Ahora bien, dado que esto no sucede, las empresas se ven en la necesidad de priorizar sus recursos y, en materia de riesgos, esto significa asignarlos de manera responsable en **orden de exposición**. Lo contrario no sólo podría delatar una gestión ineficiente, sino el malbaratamiento de recursos susceptibles de estar asignados a otros destinos preferentes. Llevado a su extremo, una asignación de recursos inadecuadamente priorizada podría ser interpretada en clave de **gestión negligente**.

Seguir una aproximación basada en el riesgo ("Risk Based Approach" –RBA-) implica asignar más recursos a **prevenir** y **detectar** los riesgos que en mayor medida exponen a la organización. Esta filosofía afecta indudablemente al modelo de *Compliance* que, lógicamente, deberá proyectarse sobre los riesgos de incumplimiento según su importancia. La consecuencia lógica de ello es el aumento de las actividades de supervisión y control con potencialidad de desencadenar incumplimientos de mayor severidad. Para ello se precisa desarrollar un *risk assessment*, como veremos más adelante en este mismo Kit, a fin de *identificar y priorizar* los riesgos de incumplimiento. Una vez realizado este ejercicio, podemos construir una **matriz de riesgos y controles** donde a cada riesgo identificado se le asigne uno o varios controles, de forma que podamos constatar, entre otras cosas, si existen riesgos apreciables sin control/es o con control/es deficiente/s. También explicaré en este Kit el modo de elaborar esa **matriz de riesgos y controles**.

El *risk assessment* constituye un ejercicio clave para seguir una **aproximación basada en el riesgo**, y su lógica termina impactando sobre la práctica totalidad de elementos del modelo de *Compliance*. A continuación te expondré un par de ejemplos para visualizar este efecto:

- La formación es un elemento importante para generar o mejorar la **cultura de cumplimiento** en las empresas. Hay quienes la consideran un **control preventivo**, puesto que contribuye a evitar que las personas incurran en riesgos de manera inadvertida o por su inadecuada percepción. Sin embargo, ni todas las personas de la organización están en disposición de provocar riesgos de incumplimiento, ni esos riesgos son los mismos para el colectivo susceptible de exponer a la empresa. Por eso, la formación: (i) no debe necesariamente impartirse a todas las personas de la organización, (ii) ni ser igual para todas ellas.

Importancia de seguir una aproximación basada en el riesgo (cont.)

Seguir una aproximación basada en el riesgo implica que, a partir de la priorización de riesgos, se identifique a los colectivos susceptibles de desencadenarlos para proyectar sobre ellos las medidas formativas oportunas.

En relación con los ciclos formativos, encontrarás ideas interesantes en el Test número 4 ("La adecuación de los ciclos formativos") de la Serie de Tests de *Compliance*.

Si consideras que una **formación selectiva** no te ayuda a generar o consolidar una cultura de cumplimiento al no abarcar a un número suficiente de personas, puedes ayudarte con acciones de sensibilización y concienciación, de alcance más general.

- Los **reportes de *Compliance*** también están afectados por la priorización, puesto que distraer a la máxima dirección en relación con riesgos inmateriales supone privar de recursos (tiempo de análisis) a otros riesgos con mayor potencialidad dañina. Los reportes de *Compliance*, tanto los operativos como las Memorias anuales, seguirán un esquema lógico de priorización respecto de las informaciones que contienen.

Hallarás más información sobre la tipología de reportes de *Compliance* en el Test número 6 ("Evaluación de los reportes de cumplimiento") de la Serie de Tests de *Compliance*.

La figura del *Compliance* Officer es esencial para el buen funcionamiento de la aproximación basada en el riesgo, pues no deja de suponer un **juicio experto** sin el cual resulta difícil ejecutar una priorización razonable. De ahí que el éxito o fracaso de la función de *Compliance* resida, en una parte nada despreciable, en la formación y **buen juicio** de las personas que encarnen la función.

Te resultarán de interés los comentarios al respecto que aparecen en el Test número 12 ("El rol del *Compliance* Officer") de la Serie de Tests de *Compliance*.

Bloques o dominios de Compliance

Todavía no es infrecuente que algunas organizaciones se pregunten qué aspectos deben quedar bajo la supervisión de *Compliance*. La respuesta dependerá de dos cuestiones, relacionadas con sus ambiciones respecto de dicha función:

- Hay organizaciones que limitan el *Compliance* al ámbito **regulatorio** de sus actividades core, siendo la aproximación tradicional de entidades que operan en **sectores regulados**. Otras organizaciones, de manera voluntaria o por imperativo legal, incrementan el alcance de *Compliance* a **cualquier norma susceptible de impactar en las operaciones**, extendiendo su ámbito de actuación sobre bloques normativos más allá de los regulados por motivo de actividad o sector.
- Otras organizaciones consideran que son obligaciones de *Compliance* tanto las que tienen carácter **obligado**, como las asumidas **voluntariamente**. A partir de ese razonamiento, que es consistente con las aproximaciones de los estándares modernos de *Compliance* (ISO 19600), esta función se ocupa de la supervisión tanto de unas como de otras.

Desde una perspectiva de control, interesa que no existan **vacíos** en materia de supervisión y que ésta se desarrolle de manera consistente. Por ello, existe la tendencia natural a concentrar el control de las obligaciones de *Compliance*, sean "*requirements*" (impuestas) o "*committments*" (voluntarias), en dicha función. Si algún día se produce un incumplimiento, no jugará a favor que concurriese en un ámbito que se excluyó del perímetro de *Compliance*.

Superestructuras de Compliance

Se utiliza el término "***Superestructura de Compliance***" cuando la función supervisa diferentes bloques de obligaciones, sea por **objeto** (obligaciones relativas a la prevención penal, a la prevención de ilícitos de competencia, a la prevención de vulneraciones de la privacidad, contra el blanqueo de capitales, etc) o por **naturaleza** (obligaciones impuestas por la Ley o los poderes públicos y obligaciones asumidas voluntariamente).

Bloques o dominios de Compliance (cont.)

En tales casos, la función de *Compliance* se convierte más en una figura de coordinación y supervisión de alto nivel, que en la gestora de las actividades de **segunda línea de defensa** que corresponden a cada uno de esos bloques o dominios, y que tienen sus respectivos responsables.

Para obtener más información puedes consultar el Test número 2 ("La adecuación de una superestructura de *Compliance*") de la Serie de Tests sobre *Compliance*.

Modelos específicos de Compliance

Los modelos específicos se proyectan sobre bloques concretos de obligaciones de *Compliance*. No pretenden una supervisión general, sino tan sólo de aquellos riesgos que guardan relación con el bloque o dominio específico. Así, por ejemplo, el modelo de prevención de blanqueo de capitales se proyectará sobre las conductas de riesgo en dicha esfera, pero no sobre otras (riesgos de corrupción, acciones de competencia ilícita, etc). Cuando no están coordinados, los modelos específicos tienden hacia una **gestión fragmentada** de *Compliance*, donde pueden multiplicarse políticas, procedimientos y controles de manera innecesaria al proyectarse sobre unos mismos hechos o procesos desde perspectivas diversas. También propician lagunas de control, si ningún modelo específico asume la supervisión de algunos riesgos de *Compliance*.

En el Cuaderno sobre cumplimiento legal número 3 ("Sistemas para la gestión del cumplimiento –CMS- Parte I") encontrarás explicadas las diferencias entre modelos específicos y genéricos de *Compliance*.

Bloques o dominios de Compliance (cont.)

Bloques o dominios según enfoque del modelo

Visto lo anterior, los bloques o dominios de ***Compliance*** dependerán del enfoque que la organización quiera darle al modelo. Existen empresas a las que sólo les preocupa un aspecto concreto de *Compliance* (cumplir con las obligaciones del regulador, evitar conductas corruptas, etc) y, entonces, optan por **acotar** su perímetro de supervisión a una o pocas materias. Otras organizaciones, sin embargo, abogan por **modelos transversales**, por superestructuras de *Compliance* que les permitan un campo de supervisión mayor y les facilite un tratamiento consistente de los riesgos de incumplimiento.

Puesto que este kit coincide con un estadio inicial del despliegue del modelo de *Compliance*, es un ejercicio que corresponde realizar ahora: no puedes avanzar en su formalización y ejecución si no tienes claro el modelo hacia el que la organización quiere avanzar. Tal vez te encuentres en una empresa que, por motivo de su tamaño y/o actividades, sólo está preocupada por dotarse de los mecanismos de prevención penal eventualmente exigidos por la normativa. Si es realmente esa su necesidad, procederá limitar el despliegue a ese ámbito específico. Pero si sus necesidades son mayores, convendrá reflexionar sobre ello para cimentar una base sólida de crecimiento del modelo. Es posible que, en este momento, debas propiciar un debate en esta materia con tu equipo directivo. En cualquier caso, toma nota de dos sugerencias que te pueden ayudar:

- Coordinar ámbitos específicos de *Compliance* a través de una superestructura no equivale a convertirse en su responsable. A través de una gestión transversal de *Compliance* se pretende racionalizar las políticas, procedimientos y controles de *Compliance*, facilitando una visión de conjunto de gran valor para la Dirección. **Pero no traslada la responsabilidad** en esos ámbitos específicos del conocimiento. Dicho en otras palabras, una superestructura facilita disponer de una segunda línea de defensa armonizada en el ámbito del *Compliance,* pero no confunde responsabilidades.

- Cuando no se dispone de ella, no es necesario implantar una superestructura de la noche al día, siendo posible hacerlo de manera **escalonada**, incorporando primero aquellas materias de mayor criticidad (aproximación basada en el riesgo) para luego hacer lo propio con las restantes.

Finalmente, ten en cuenta que el alcance del modelo de *Compliance* es algo que tendrá reflejo tanto en la **Política de *Compliance*** como en la representación documental del resto del *Compliance* Management System (CMS), según expliqué en el Kit anterior.

Concreción del órgano de Compliance

Lógicamente, la composición del órgano de *Compliance* guarda relación con el alcance de la función. Veamos algunas consecuencias que se derivan de ello.

Obtendrás información útil sobre el órgano de *Compliance* en el Cuaderno sobre cumplimiento legal número 3 ("Sistemas para la gestión del cumplimiento –CMS- Parte I") y en el Test número 10 ("Evaluación del modelo de prevención penal español – El órgano de prevención penal"), en relación este último con los modelos de prevención de delitos españoles.

También encontrarás reflexiones interesantes, derivadas de malentendidos clásicos, en el Caso número 12 ("Cuando la función de *Compliance* la desarrolla un órgano colegiado") de la Serie sobre Errores de *Compliance*. Verás que Stephen, el *Compliance* Officer de una organización, incurre en varios errores conceptuales y de comunicación cuando pretende migrar un modelo anti-corrupción a otro de alcance mayor.

Órgano colegiado vs órgano unipersonal

En superestructuras de *Compliance*, tiene sentido que estén representados los máximos responsables –y conocedores- de cada uno de los bloques de cumplimiento o dominios coordinados por la función. Esto no significa que necesariamente deban formar parte de dicho órgano, aunque es una circunstancia que normalmente incrementa su nivel de compromiso.

En líneas generales, los modelos de *Compliance* complejos tienden a figuras orgánicas **colegiadas**, mientras que los más sencillos (modelos específicos) se asocian a figuras **unipersonales**, con independencia del soporte administrativo y técnico que tengan tanto unas como otras. Los estándares modelos sobre *Compliance* han sustituido expresamente el vocablo "*Compliance* Manager" –o equivalentes- por el de "*Compliance* function", para reconocer esta **diversidad**. No obstante, es posible

Concreción del órgano de Compliance (cont.)

que localices normas que se refieren al *Compliance* Officer (utilizando nomenclatura diversa), normalmente en el contexto de campos específicos del cumplimiento. En esos casos, deberás articular el encaje de ese requisito normativo en el contexto de tu modelo de *Compliance*, para que dé respuesta tanto a las exigencias legales como a los objetivos de la organización. Ese encaje es normalmente sencillo, pues la atribución de ciertas competencias por motivo de especialidad a un *Compliance* Officer (CO), no está necesariamente reñida con su integración en un órgano colegiado con un Presidente o un Chief *Compliance* Officer (CCO). De hecho, la figura del CCO adquiere pleno sentido cuando concurren varios COs con atribuciones en ámbitos de cumplimiento específicos.

Evolución de modelos

Algunas empresas comienzan disponiendo de órganos de *Compliance* adecuados para modelos modestos (normalmente específicos, sobre un bloque de cumplimiento), para luego plantearse la migración a modelos de **mayor valor añadido**. Esta circunstancia puede impactar en la composición del órgano de *Compliance*, de modo que tendrás que prever su evolución cuando su punto de partida haya sido sencillo. Plantéate si la composición inicial del órgano de *Compliance* podrá mantenerse al aumentar sus competencias, y presta atención en no establecer barreras que dificulten esa transformación el día de mañana.

El outsourcing y el co sourcing

Puede ocurrir que organizaciones pequeñas no estén expuestas a riesgos que justifiquen estructuras de *Compliance*, ni dispongan de recursos para implantarlos. En tales escenarios, y cuando no deseen renunciar al objetivo de una gestión respetuosa con el cumplimiento de las normas, es razonable que se planteen la posibilidad de **externalizar** alguno de los cometidos de esa función ("outsourcing"). Siempre que no esté prohibido, es una opción a valorar, que ya se ha dado en países de nuestro entorno, aunque no evita que el sujeto afectado por las obligaciones de *Compliance* siga siendo la empresa.

Otras organizaciones optan por no externalizar cometidos de *Compliance* pero se auxilian de colaboradores externos que les ayudarán a incorporar criterio experto ("co sourcing"). Es un esquema que multiplica las capacidades internas sin incrementar los costes fijos, normalmente asociados a las nuevas contrataciones de personal. Es también una opción recurrida en los momentos de **despliegue inicial** del modelo.

Obviamente, algunas organizaciones conjugan el *outsourcing* y el co-sourcing.

Dependencia funcional

Definido el órgano de *Compliance*, tendrás que plantearte su dependencia funcional, esto es, de qué órgano superior depende y al que rinde cuentas.

Está generalmente aceptado que la función de *Compliance* precisa cercanía

Concreción del órgano de Compliance (cont.)

a los máximos órganos de dirección por un motivo de eficacia, pues sólo de esta manera se facilita una comunicación fluida con los mismos y se fijan los fundamentos sobre los que asentar su **independencia y autonomía**. Esto conduce a plantear normalmente **dependencias funcionales** directas del órgano de administración social, o de comisiones delegadas del mismo. No es inhabitual que el órgano de *Compliance* dependa directamente del Consejo de Administración, por ejemplo. No obstante, en sociedades cotizadas, suele depender de comisiones delegadas especializadas donde participan consejeros independientes, como pueden ser las de Auditoría (que, en ocasiones adquiere la denominación de "Comisión de Auditoría y Cumplimiento"). Salvo restricciones legales, esto no es óbice para establecer la dependencia funcional a otra **comisión delegada** distinta, según las que haya autorregulado el Consejo de Administración (Reglamento Interno del Consejo –RIC-) y las competencias otorgadas a las mismas.

Transversalidad de la gestión de riesgos

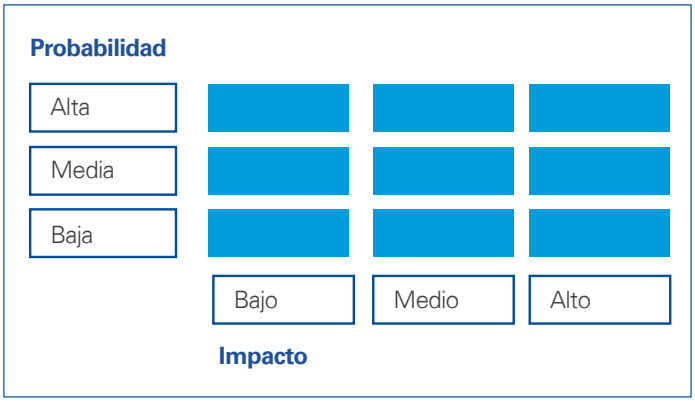
En el Kit número 1 de esta Serie apunté la conveniencia de conectar los cometidos de *Compliance* con otros fuertemente **sinérgicos**, como los propios de la **gestión de riesgos**. Procede ahora incidir en ello, antes de que desarrolles el ***risk assessment*** según las directrices del apartado siguiente de este Kit.

Existen diversas metodologías para la **valoración de riesgos**, sin que los estándares de *Compliance* se decanten por alguna de ellas en particular (la norma ISO 19600 cita la metodología de riesgos descrita en la norma ISO 31000 pero no obliga a utilizarla). Tiene sentido que así sea por cuanto sistemáticas complejas pueden entrañar una dificultad excesiva para empresas pequeñas y medianas, mientras que sistemáticas simples se pueden antojar deficientes para las grandes. En definitiva, cada organización es libre de seleccionar la metodología de valoración de riesgos que mejor se adapta a sus circunstancias, ¡aunque puede tener que dar cuentas de ello en algún momento!

Así las cosas, recuerda que los riesgos de incumplimiento sólo son una parte de los riesgos que afronta cualquier organización, siendo susceptibles de ser evaluados bajo el mismo rasero que el resto. Por motivo de especialidad, tiene sentido que *Compliance* tenga una participación o incluso el protagonismo en la valoración de los **riesgos de incumplimiento**, pero esto no justifica utilizar una metodología de medición independiente que dificulte **contextualizarlos** con el resto. Por este motivo, antes de iniciar el ejercicio de *risk assessment* y desarrollar la posterior matriz de riesgos y controles, es importante conocer qué **metodología** utiliza tu organización para aplicarla correctamente.

Transversalidad de la gestión de riesgos (cont.)

Cuando profundices acerca de la metodología a utilizar, identificaras **criterios** relevantes a la hora de desarrollar un risk assessment coherente con el resto de materias, y que pueden incidir en la escala de valoración, aspectos a considerar para concretar la puntuación dentro de dicha escala, taxonomía utilizada para identificar los riesgos, nomenclatura de controles según tipología, etc. Así, por ejemplo, una organización puede valorar sus riesgos en una escala de tres magnitudes (bajo, medio y alto), mientras que otra puede recurrir a cinco (muy bajo, bajo, medio, alto y muy alto) o incluso más. Aplicando este baremo tanto a la **probabilidad** como al **impacto**, puede resultar una matriz de 9 posiciones en el esquema simple, mientras que será de 25 en la versión extendida.



Transversalidad de la gestión de riesgos (cont.)

Los riesgos a los que hay que prestar **atención prioritaria** son aquellos que se concentran en las posiciones próximas o equivalentes a la superior derecha, mientras que los **menos relevantes** ocupan posiciones próximas o equivalentes a la inferior izquierda.

Desarrollar un *risk assessment* de *Compliance* alineado con la metodología y criterios de valoración de riesgos de la organización favorece su **integración** y mejora su visibilidad.

Risk Assessment

Recurriendo al adagio "nunca soplan buenos vientos para quien no sabe a dónde va", podríamos decir que el *risk assessment* es la piedra angular de cualquier modelo de gestión basado en el riesgo. Sin este ejercicio, difícilmente pueden determinarse medidas de prevención y detección adecuadamente enfocadas, y el órgano de *Compliance* corre el riesgo de dar palos de ciego. Por eso, en teoría, antes de documentar un modelo de *Compliance* deberían conocerse los **riesgos** sobre los que se proyectará.

Paradójicamente, los estándares de *Compliance* modernos suelen referirse al *risk assessment* como parte esencial de los modelos que describen, situándolo en un estadio coetáneo o posterior a la definición del propio modelo.

Algunas normas de *Compliance*, como el IDW Asss 980, apuntan la posibilidad de desarrollar el ejercicio de *risk assessment* mediante un doble análisis inicial: identificando los **bloques de cumplimiento** o dominios dentro del perímetro de *Compliance*, para luego concretar las **casuísticas de riesgo** asociadas a cada uno de ellos. Así, por ejemplo, siendo la protección de la privacidad un dominio de *Compliance*, una de las diversas casuísticas de riesgo asociadas al mismo sería la cesión de datos personales a terceros sin observar las previsiones exigidas legamente.

Constituye una opción clásica valorar el riesgo asociado a cada casuística en término de **probabilidad** e **impacto**. También se puede concretar la severidad del riesgo, como valor resultante de los dos parámetros anteriores.

Encontrarás comentarios detallados acerca del risk assessment en el Test número 9 ("Evaluación del modelo de prevención penal español – Risk Assessment") de la Serie de Tests de Compliance. Aunque este documento se circunscribe a los modelos de prevención penal en España, sus conclusiones son extrapolables para otros entornos.

Un *risk assessment* así ejecutado te facilitará identificar las **actividades** e incluso los **procesos** de la empresa potencialmente afectados por los riesgos, así como los **colectivos de personas** próximos a ellos. Como explicaré en el apartado siguiente, a partir de ahí podrás valorar la suficiencia de los controles sobre ambos y obrar en consecuencia. Existen metodologías de consultoría que invierten el orden de trabajo, identificando los procesos de la organización para detectar los riesgos y controles asociados a cada uno de ellos. Las conclusiones así alcanzadas deberían ser idénticas, salvo que existan riesgos

Risk Assessment (cont.)

de *Compliance* asociados con actividades huérfanas todavía de un proceso identificado como tal.

La plasmación gráfica del risk assessment será un mapa de riesgos de *Compliance*, donde se ubicarán los diferentes bloques y sus casuísticas según **probabilidad** de comisión e **impacto**.

De cara a documentar el *risk assessment*, no olvides recoger, además de la propia **conclusión** en cuanto a la probabilidad de ocurrencia de los riesgos y su impacto para la organización, **quién** ha llegado a tal conclusión, **cuál** ha sido el razonamiento para llegar a ella y, finalmente, a que **procesos** o **colectivos** de la empresa afecta el **riesgo**.

Matriz de riesgos y controles

Ahora que has desarrollado el ***risk assessment*** y dispones de una priorización de riesgos, puedes ocuparte de analizar los controles que existen para su prevención y detección. Prepárate para elaborar una **matriz de riesgos y controles**.

Para cada bloque de cumplimiento o dominio dentro del perímetro de *Compliance* (llamado en ocasiones "Universo de *Compliance*") lista las casuísticas de riesgo según la prioridad resultante del *risk assessment*. Cada **casuística** debería tener asociado uno o varios **controles**. De hecho, cuanto mayor es la severidad de un riesgo, más robusto y/o mayor número de controles deberían vincularse con él. Por eso, no es infrecuente que las matrices de riesgos y controles muestren una simplificación de contenidos a medida que se abordan casuísticas poco relevantes.

Puedes realizar este ejercicio en forma de tabla, de modo que a cada bloque de *Compliance* o dominio y sus respectivas casuísticas, además de su calificación (priorización) y control/es asociado/s, les asignes información adicional de utilidad, resultando, por ejemplo:

- Bloque o dominio de *Compliance*.
- Descripción de la casuística.
- Identificación de la persona jurídica en la que se puede producir (relevante en grupos empresariales).
- Calificación del riesgo bruto (sectorial) de esa casuística.
- Identificación de los controles vinculados a esa casuística.
- Calificación de la naturaleza de cada control (preventivo o detectivo, por ejemplo).
- Calificación del tipo de control (automatizado o manual, por ejemplo).
- Frecuencia de cada control.
- Propietario de cada control.
- Juicio de evaluación sobre el diseño de cada control.
- Valoración de la efectividad de cada control.
- Riesgo neto (de la organización, considerando sus controles) de esa casuística.

La matriz de riesgos y controles se puede enriquecer con mucha más información, conforme a la idiosincrasia de cada organización y sus necesidades. Es más, **pueden asignarse valores numéricos** a muchos de los elementos que aparecen en la relación anterior, de modo que la traslación de **riesgo bruto a riesgo neto** derive de una operación matemática (aumentando el efecto matemático de los controles automáticos sobre los manuales, de los frecuentes respecto de los que no lo son, etc). Cuanto más completa y detallada sea la información contenida en este documento, más se facilitará la eventual labor de auditoría del modelo. Dedicaré el Kit número 11 de esta Serie a hablar de ello.

Y ahora... ¿qué hago?

Una vez asimilado el contenido de este kit, ha llegado el momento de que te pongas manos a la obra y, para ello, te facilito a continuación algunas sugerencias.

Acciones a desarrollar durante la tercera semana

Organiza entrevistas con los responsables de materias susceptibles de coordinación a través de la función de *Compliance*. Si en estas entrevistas detectas opiniones no alineadas con las atribuciones u objetivos del modelo de *Compliance*, coméntalo con la persona u órgano que esté impulsando el proyecto y clarifica la situación antes de continuar.

Con la información obtenida, identifica los bloques normativos susceptibles de incorporarse dentro del perímetro de supervisión de la función, y su criticidad.

Sobre la base de lo anterior, define la composición del órgano de *Compliance* y su estructura interna. También plantea cuál será su dependencia funcional. Necesitarás esta información para concluir la documentación del Modelo de *Compliance*, la próxima semana.

Desarrolla un *risk assessment* en relación con los bloques normativos o dominios supervisados por *Compliance*. Aprovecha la metodología que venga utilizando la organización. El *risk assessment* que elabores te debe permitir priorizar los riesgos que hayas identificado.

Tomando como partida el *risk assessment* de *Compliance*, elabora una matriz de riesgos y controles donde figuren de manera priorizada las casuísticas de riesgo asociadas a cada bloque normativo o dominio, así como los controles asociados a cada una de ellas. Contrasta la suficiencia de los controles considerando la priorización de las casuísticas.

Serie

Kits de despliegue de *Compliance*

Kit 1

Plan de acción para la primera semana
Puesta en contexto y ubicación

La función de *Compliance* no actúa de manera aislada, sino que interactúa necesariamente con otras funciones clave en el seno de la organización, contribuyendo a articular las famosas tres líneas de defensa. Este kit te ayudará a dar los primeros pasos para adquirir unos fundamentos sólidos acerca de los cometidos de *Compliance* y comenzar a definir relaciones con esas funciones sinérgicas, sin las cuales será difícil que desarrolles eficazmente tu labor y que la organización alcance sus objetivos de *Compliance*.

Kit 2

Plan de acción para la segunda semana
Documentando la función y aspectos personales importantes

Existen diversos motivos por los cuales es importante documentar adecuadamente la función de *Compliance*. Este kit te permitirá conocer los aspectos clave a considerar a tales efectos, de forma que quede constancia de su existencia y pueda validarse la idoneidad de su diseño. También te facilitará información de utilidad para que puedas desarrollar tu cometido en un marco razonable de seguridad personal.

Kit 3

Plan de acción para la tercera semana
Aproximación basada en el riesgo del modelo y cuestiones organizativas

Los estándares más modernos en materia de *Compliance* siguen una aproximación basada en el riesgo. Por consiguiente, es importante que conozcas qué significa esto y cómo se traslada a los componentes que conforman el modelo de *Compliance*. Este kit también te ayudará a diseñar aspectos organizativos clave del modelo que le permitirán operar eficazmente.

Serie - Kits de despliegue de *Compliance* (cont.)

Kit 4

Plan de acción para la primera semana
Terminando de documentar el modelo y los procesos de diligencia debida

Una vez desarrolladas las recomendaciones de los kits anteriores, se puede completar la representación documental del modelo en sus extremos más significativos. Este kit te permitirá concluir el trabajo iniciado en el Kit 1, y familiarizarte con algo muy importante en todo modelo de *Compliance*: los procesos de diligencia debida en relación con las personas con las que se vinculan con la organización. Conocerás las formas de segmentar esos procedimientos para que no se conviertan en un gravamen inútil.

Kit 5

Plan de acción para la quinta semana
Primera ronda de diligencia debida y bases de generación de una cultura de cumplimiento

Una vez definidos los procedimientos de diligencia debida relativos a *Compliance* procede su ejecución, de la cual derivarán algunos planes de acción. Este kit te ayudará en esas labores, y también a que prestes atención y desarrolles algunos aspectos que los estándares más modernos de *Compliance* consideran básicos para establecer, mejorar o consolidar la cultura de cumplimiento de la organización.

Kit 6

Plan de acción para la sexta semana
Escalado y plan de revisiones de *Compliance*

El modelo de *Compliance* contemplará mecanismos de escalado en diferentes sentidos: los que permiten que cualquier interesado acceda a la función para comunicar sus inquietudes o solicitar consejos, así como los que afectan a la propia función de *Compliance* respecto de los órganos de máxima responsabilidad social. Este kit te facilitará definir tales mecanismos y también te explicará la necesidad de articular y ejecutar un plan de revisiones de *Compliance*.

Serie - Kits de despliegue de *Compliance* (cont.)

Kit 7

Plan de acción para la séptima semana
Despliegue del modelo de *Compliance*: plan y priorización

Cuando una organización opera en diversos emplazamientos, debería plantearse el modo de desplegar su modelo de *Compliance* en ellos. Este kit te ayudará a considerar diversos factores que son relevantes a la hora de definir el nivel de centralización o descentralización del modelo, así como para elaborar un modelo fácilmente desplegable. También encontrarás ideas para priorizar el plan de despliegue, para el caso en que sea materialmente imposible ejecutarlo en unidad de acto.

Kit 8

Plan de acción para la octava semana
Check-list y plan de visitas

La función de *Compliance* se ocupará de diseñar protocolos de revisión interna que faciliten comprobar si los distintos emplazamientos de la organización asumen adecuadamente los cometidos que les atribuye el Sistema de Gestión de *Compliance* (CMS). Para ello, se precisa un notable grado de movilidad, de forma que la función pueda satisfacerse razonablemente de su nivel de comprensión y ejecución, pudiendo así detectar y corregir debilidades a tiempo. Este kit te ayudará, por lo tanto, a comprobar el despliegue efectivo del modelo de *Compliance*.

Kit 9

Plan de acción para la novena semana
Reportes operativos de *Compliance* y memorias anuales

La función de *Compliance* debe reportar sus actividades de forma recurrente a la máxima dirección. Igualmente, el resultado de su labor quedará plasmado en memorias anuales susceptibles de ser integradas en otros reportes de gestión de mayor alcance. Este kit te brindará ideas sobre los contenidos tanto de los reportes operativos como de las memorias anuales, permitiendo identificar KRI's de *Compliance* y valorar su evolución.

Serie - Kits de despliegue de *Compliance* (cont.)

Kit 10

Plan de acción para la décima semana
Ejecución de acciones correctoras de *Compliance*

El concepto de "información documentada" aplicada al ámbito del *Compliance* no se limita a la documentación básica que representa el modelo, sino también a la que resulta de su aplicación práctica. Por lo tanto, la existencia y ejecución de los planes de acción derivados de incidentes relacionados con el *Compliance* forman una parte importante de la información documentada a elaborar y custodiar, cuyo contenido te ayudará a definir este kit.

Kit 11

Plan de acción para la décimo primera semana
Ejecución de revisiones de *Compliance*

Habiendo sido definidas previamente (kit 6), procede desarrollar las revisiones del modelo de *Compliance*, para lo cual se precisarán recursos internos y/o externos. En este kit encontrarás diferentes aspectos que puedes valorar a la hora de lanzar un procedimiento de verificación de *Compliance*, como el outsourcing o el co-sourcing, planificando razonablemente los recursos y tiempo que vas a precisar en virtud de la opción que elijas.

Kit 12

Plan de acción para la décimo segunda semana
Acercando *Compliance* a los grupos de interés

La función de *Compliance* no puede evolucionar alejada de los grupos de interés (stakeholders) de la organización, ya que buena parte de las obligaciones y compromisos de *Compliance* traen causa en ellos. La función de *Compliance* está llamada a convertirse en el interlocutor de la empresa con sus grupos de interés, incluidas las administraciones públicas. En este kit encontrarás ideas para avanzar hacia ese objetivo.

Bibliografía del autor

Legal *Compliance* **- Principios de Cumplimiento Generalmente Aceptados**
Alain Casanovas

Prólogo de José Manuel Maza, Magistrado del Tribunal Supremo
Editor, Grupo Difusión
Difusión Jurídica y Temas de Actualidad, S.A.
Madrid 2013

Control Legal Interno
Alain Casanovas

Prólogo de Pedro Mirosa, *Catedrático de Derecho Mercantil, ESADE, Factultad de Derecho*

Editor Grupo Wolters Wluwer
Editorial La Ley, S.A.

Madrid 2012

Control de Riesgos Legales en la empresa
Alain Casanovas

Prólogo de Lord Daniel Brennan Q.C., former President of the Bar of England and Wales

Editor Grupo Difusión
Difusión Jurídica y Temas de Actualidad, S.A.

Madrid 2008

Obra digital del autor

Tests de *Compliance*
Alain Casanovas
www.kpmgcumplimientolegal.es
Madrid 2015

Casos sobre errores de *Compliance*
Alain Casanovas
www.kpmgcumplimientolegal.es
Madrid 2014

Cuadernos sobre Cumplimiento Legal
Alain Casanovas
www.kpmgcumplimientolegal.es
Madrid 2013

Contacto

Alain Casanovas
Socio de KPMG Abogados
T: +34 93 253 29 22
E: acasanovas@kpmg.es

Perfil en LinkedIn

www.kpmgcumplimientolegal.es