Directrices finales sobre gobierno interno en el marco de la CRD

EBA/GL/2021/05

Lista de abreviaturas

Abreviaturas	Significado
EBA	European Banking Authority
GL	Guidelines
CRD	Capital Requirements Directiv
IFD	Investment Firms Directive
CA	Competent Authorities
RMF	Risk Management Function
AMA	Métodos de Medición Avanzada
AMLD	Directiva 2015/849/EU relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo
G-SIIs	Entidades de importancia sistémica mundial
O-SIIs	Otras Entidades de importancia sistémica

Índice

Introducción

En julio de 2021, la EBA publicó las GL finales sobre gobierno interno, que actualizan las GL existentes publicadas en 2017. La actualización tiene en cuenta las modificaciones introducidas por la CRD y la IFD en relación con los acuerdos de gobernanza eficaces y sólidos de las entidades de crédito.

Introducción

Durante los últimos años, el marco de gobierno interno de las entidades ha recibido una mayor atención por parte de diversos organismos internacionales. En este sentido, su principal esfuerzo ha sido corregir las deficiencias identificadas en las prácticas de gobierno interno, dado que algunas de estas prácticas se han observado inapropiadas y, aunque no hayan sido un desencadenante de la crisis financiera, estaban relacionadas con la misma y eran cuestionables.

De conformidad con la CRD IV, la EBA tiene encomendada la armonización de los mecanismos, procesos y disposiciones relativas al gobierno interno de las entidades dentro de la EU. En este sentido, en septiembre de 2011 la EBA publicó Directrices sobre gobierno interno (GL 44) con el objetivo de mejorar y consolidar expectativas supervisoras, así como fortalecer el marco de gobierno interno.

En 2017, la EBA actualizó las GL 44 con objeto de seguir armonizando los acuerdos, procesos y mecanismos de gobernanza interna de las entidades en toda la EU. Estas directrices ponen más énfasis en las obligaciones y responsabilidades del órgano de dirección en su función de supervisión del riesgo.

- En este contexto, tras la consulta iniciada en diciembre de 2021, la EBA publicó **Directrices Finales sobre gobierno interno** que actualizan las GL 44 y se centra en la diversidad de género, el blanqueo de capitales, el riesgo de financiación del terrorismo y la gestión de los conflictos de intereses, incluso en el contexto de los préstamos y otras transacciones con los miembros del órgano de dirección y sus partes vinculadas. En particular, este documento cubre los siguientes aspectos:
  - El rol y la composición del **órgano de dirección y comités** (de riesgos, de nombramientos y de remuneraciones).
  - El **marco de gobierno**.
  - La **cultura de riesgo** y **conducta de negocio**.
  - El marco y mecanismos de **control interno**.
  - La **gestión de la continuidad del negocio**.
  - Los principios de **proporcionalidad** y **transparencia**.

Este documento incluye un **análisis de los requerimientos** de las Directrices finales sobre gobierno interno.

Índice

Resumen ejecutivo

Estas GL incluyen disposiciones sobre: i) el rol del órgano de dirección y de los comités; ii) marco de gobierno; iii) cultura de riesgo y conducta de negocio; iv) control interno; v) gestión de continuidad del negocio; y vi) principios aplicados al marco de gobierno interno

Resumen ejecutivo

Ámbito de aplicación

- Estas directrices están dirigidas a **entidades de crédito** y **empresas de servicios de inversión**, según los define el CRR.

Contexto regulatorio

- **Directrices sobre gobierno interno** (GL 44), publicadas por la EBA en septiembre de 2011 y actualizadas en 2017.

Próximos pasos

- Estas GL se aplicarán a partir del **31 de diciembre de 2021** a las CA y a las entidades.
- Las GL publicadas en 2017 serán derogadas en la **misma fecha.**

Contenido principal

Órgano de dirección y comités

- Deberes y responsabilidades del órgano de dirección, función supervisora y función de gestión, presidente del órgano de dirección, marco organizativo y estructura, y comités.

Marco de gobierno

- Marco organizativo y una estructura adecuados y transparentes, en un contexto de grupo, y con una política de externalización que considere el impacto de la externalización sobre el negocio de la entidad y los riesgos de la entidad.

Cultura del riesgo y cultura de negocio

- Cultura de riesgos integrada e institucional basada, entre otros, en los riesgos a los que está expuesta; conflictos de intereses, procedimientos de alerta interna y notificación a las CA.

Marco y mecanismos control interno

- Marco de control interno y gestión de riesgos, nuevos productos, funciones de control interno (responsables y recursos), y funciones concretas de RMF[1], cumplimiento y auditoría interna.

Gestión de continuidad de negocio

- Implementación de una sólida gestión de continuidad de negocio por parte de las entidades para reducir las consecuencias derivadas de un fallo o una interrupción extendida sobre recursos críticos.

Principios aplicados a gobierno interno

- Principios de proporcionalidad (en función del tamaño, organización interna y la naturaleza y complejidad de sus actividades) y transparencia aplicados por las entidades al definir su marco de gobierno interno.

(1) Función de gestión de riesgos

Índice

Detalle

Rol y composición del órgano de dirección y comités

Estas GL ofrecen orientaciones sobre los deberes y responsabilidades del órgano de dirección, los cuales deben definirse distinguiendo entre la función supervisora…

Órgano de dirección y comités (1/4)

Deberes y responsabilidades

- El órgano de dirección debe ser el **máximo responsable** de la entidad y definir, supervisar y ser responsable de la implementación de mecanismos de gobierno. Asimismo, se deben definir claramente sus deberes, distinguiéndose entre aquellos de los **miembros ejecutivos**[1] y de los **miembros no ejecutivos**[2]. Todos los miembros deben conocer la estructura y las responsabilidades del órgano de dirección, así como el reparto de tareas entre las diferentes funciones del órgano de dirección y sus comités.
- Los deberes y responsabilidades del órgano de dirección deben describirse en un **documento escrito** y aprobado por el órgano de dirección, debiendo incluir el establecimiento, aprobación y control de la implementación de, entre otros:
  - La **estrategia global** y la **estrategia de riesgo global** (ej. apetito al riesgo, marco de gestión de riesgos).
  - Un **marco de control interno** adecuado, efectivo e independiente y garantizar el cumplimiento de los requisitos normativos aplicables en el contexto de la prevención del blanqueo de capitales y la financiación del terrorismo.
  - Los importes, tipos y distribución del capital interno y del capital regulatorio.
  - Una **política de remuneración** en línea con esta GL.
  - Mecanismos que garanticen la **evaluación de la idoneidad individual** y **colectiva del órgano de dirección**.
  - Mecanismos destinados a garantizar el funcionamiento interno de cada **comité**.
  - Una **cultura de riesgo** y **corporativa** adecuados.

Función de gestión

- El órgano de dirección debe supervisar el proceso de **divulgación y comunicación** y sus miembros deben estar informados sobre la actividad global, la situación financiera y de riesgo de la entidad. Además, deben monitorizar y **revisar periódicamente** cualquier debilidad identificada en la implementación de procesos, estrategias, etc. Además, deben incluir un marco de gestión de riesgos que tenga en cuenta los factores de riesgo ESG y considerar que los riesgos de gobernanza pueden impulsar los riesgos prudenciales y los riesgos de crédito.

- El órgano de dirección debe **participar activamente en el negocio** de la entidad y debe **tomar decisiones** sobre una base sólida y bien informada.

(1) Miembros del órgano de dirección en su función de gestión.
(2) Miembros del órgano de dirección en su función de supervisión.

Detalle

Rol y composición del órgano de dirección y comités

…y la función de gestión. Además, las GL también ofrecen orientaciones sobre el rol del presidente del órgano de dirección como principal responsable de su funcionamiento efectivo

Órgano de dirección y comités (2/4)

Función de gestión

- La función de gestión del órgano de dirección implica, entre otras cosas:
  - Aplicar las **estrategias establecidas** por el órgano de dirección y debatir periódicamente sobre su aplicación e idoneidad.
  - **Cuestionar de forma constructiva y revisar** de forma crítica las propuestas, explicaciones e informaciones recibidas, a la hora de aplicar su criterio y tomar decisiones.
  - Identificar a uno de sus miembros como responsable de la aplicación de la normativa de la AMLD.

Función supervisora

- El órgano de dirección debe, entre otros:
  - Controlar y **consultar constructivamente la estrategia** de la entidad, supervisar al órgano de dirección en su función de gestión, incluida la supervisión y el control de su desempeño individual y colectivo.
  - Evaluar periódicamente la eficacia de su **marco de gobierno interno**.
  - Supervisar la implementación de la **cultura de riesgo, el plan de auditoria** y los objetivos estratégicos de la entidad así como la integridad de la información financiera y la presentación de informes.
  - Asegurar que los jefes de las funciones de control interno pueda actuar **independientemente** de otros órganos internos.
  - Supervisar la implementación y mantenimiento de un código de conducta o políticas similares y efectivas para identificar gestionar y mitigar los **conflictos de intereses** reales y potenciales.

Presidente del órgano de dirección

- El presidente debe liderar el órgano de dirección y contribuir al **flujo eficiente de información** dentro del órgano de dirección, y entre el órgano de dirección y sus comités; debe ser el **responsable de su funcionamiento efectivo;** así como debe fomentar y **promover debates abiertos y críticos** para garantizar que se pueden manifestar opiniones divergentes.
- Como principio general, el presidente debe ser un miembro **independiente o no ejecutivo**. Por lo tanto, el presidente en su función supervisora y el **CEO de un entidad no deben ser la misma persona**, a menos que esté justificado por la entidad y autorizado por la CA.
- El presidente debe, entre otras funciones:
  - Fijar la **agenda de reuniones** y garantizar que los problemas estratégicos se discuten con prioridad.
  - Garantizar una **clara asignación de responsabilidades** entre miembros ejecutivos y no ejecutivos del órgano de dirección, así como la existencia de un flujo eficiente de información entre los mismos.

Detalle

Rol y composición del órgano de dirección y comités

Además, proporcionan guías sobre los comités, en particular en lo relativo a su creación, composición y procesos

Órgano de dirección y comités (3/4)

Comités

- Todas las entidades que son **sistémicas**[1] (a nivel individual, subconsolidado y consolidado) deben establecer un **comité de riesgos, de nombramientos y de remuneración** para asesorar al órgano de dirección en su función supervisora[2].
- Las **entidades no significativas**, incluidas aquellas que se encuentren dentro del ámbito de la consolidación prudencial de entidades significativas a nivel subconsolidado o consolidado, **no están obligadas a establecer dichos comités**. Cuando no se establezcan comités de riesgos o de nombramientos, dichos comités deberán atribuirse al órgano de dirección en su función de supervisión.
- Las entidades pueden establecer **otros comités especializados** (ej. la lucha contra el blanqueo de capitales y la financiación del terrorismo (AML/CTF), comités de ética, conducta y cumplimiento).
- En relación con la **composición de los comités**:
  - Todos los comités tiene que estar presididos por **un miembro no ejecutivo** del órgano de dirección, estar compuestas por al menos **tres miembros**, y no estar integrados por el mismo grupo que el previsto en otro comité.
  - Las entidades deben considerar la **rotación ocasional de los presidentes** y de los miembros de los comités, considerando su experiencia, conocimientos y habilidades específicas.
  - Los comités de riesgos y de nombramientos deben estar compuestos por **miembros no ejecutivos**.
  - Además, en las **G-SII y O-SII** estos comités deben estar compuestos, en su mayoría por miembros independientes, y estar presidido por un miembro independiente.
  - En **otras entidades significativas**, determinadas por las CA o por la legislación nacional, los comités de riesgos deben ser presididos, cuando sea posible, por un miembro independiente.
  - En **todas las entidades**, el presidente del comité de riesgos no debe ser ni el presidente del órgano de dirección ni el presidente de ningún otro comité.
- Asimismo, los comités deben informar periódicamente al órgano de dirección en su función de supervisión, tener acceso a toda la información relevante y a todos los datos necesarios, etc.

(1) Entidades de importancia sistémica global o 'G-SII', otras entidades de importancia sistémica u 'O-SII', y otras entidades identificadas como tal por las CA.
(2) Las entidades no sistémicas podrían establecer un único comité con ambas funciones.

Detalle

Rol y composición del órgano de dirección y comités

Las GL también especifican los deberes de los comités de riesgos, de auditoria, así como de los comités combinados

Órgano de dirección y comités (4/4)

Comité de riesgos

- Entre otras funciones, este comité debe:
  - Asesorar y apoyar al órgano de dirección en su función supervisora respecto a la monitorización del **apetito al riesgo** global de la entidad y la **estrategia**, considerando todos los tipos de riesgo.
  - Asistir al órgano de dirección en su función supervisora respecto a la implementación de la **estrategia de riesgo** de la entidad y de sus correspondientes **límites** fijados.
  - Supervisar la implementación de las estrategias para la **gestión de capital y liquidez** y para todos los riesgos relevantes restantes de una entidad (ej. mercado, crédito, operacional y reputacional).
  - Proporcionar **recomendaciones** sobre los ajustes necesarios en la estrategia de riesgo.

Comité de auditoria

- Entre otras funciones, este comité debe:
  - Monitorizar la efectividad del **control de calidad interno** de la entidad, de los **sistemas de gestión del riesgo**, y cuando corresponda, de su **auditoría interna**.
  - Supervisar el establecimiento de **políticas contables** por parte de la entidad.
  - Monitorizar el **proceso de reporting financiero** y dar recomendaciones para garantizar su integridad.

Comités combinados

- Las CA pueden permitir a entidades no consideradas significativas la **combinación del comité de riesgo y**, cuando así lo establezcan, **del comité de auditoria**.
- Cuando se creen comités de riesgos y de nombramientos en **entidades no significativas**, dichas entidades podrán combinar estos comités. En dicho caso, estas entidades deben documentar las razones por las cuales han optado por combinar estos comités, así como el enfoque previsto para alcanzar los objetivos de los comités.
- Las entidades deben garantizar en todo momento que los miembros de un comité combinado ostentan, individual y colectivamente, los **conocimientos, aptitudes y experiencia** necesarios.

Detalle

Marco de gobierno

De acuerdo con estas GL, el órgano de dirección debe garantizar un marco organizativo y una estructura adecuados y transparentes y tener una descripción escrita de ello. En este sentido, debe evitar el establecimiento de estructuras complejas y se debe considerar la aplicación de medidas de mitigación

Marco de gobierno (1/2)

Marco organizativo y estructura[1]

- En relación con el **marco organizativo**, el órgano de dirección debe:
  - Garantizar que la estructura promueva y demuestre la gestión **eficaz y prudente** de una institución.
  - Garantizar el mayor nivel de **independencia posible de las funciones de control interno**, considerando los recursos financieros y humanos necesarios para realizar sus funciones de manera efectiva. Las líneas de información y la asignación de responsabilidades, en particular entre los titulares de funciones clave, deben ser claras, coherentes, bien definidas, ejecutables y bien documentadas.
  - Supervisar y gestionar eficazmente los **riesgos a los que se enfrenta la entidad o el grupo**, o la capacidad de la CA para ejercer una supervisión eficaz de la entidad.
  - Evaluar cuales son y cómo se aplican los **cambios materiales** en la estructura del grupo (ej. establecimiento de nuevas filiales, fusiones y adquisiciones, etc.).

- Con respecto a la **estructura**, el órgano de dirección debe:
  - Conocer y entender plenamente la estructura organizativa y operativa (**know-your-structure**) y garantizar que está en línea con el negocio, estrategia de riesgo ,apetito al riesgo y que está cubierto por su **marco de gestión de riesgos.**
  - Ser responsable de la **aprobación de estrategias y políticas sólidas**.

- Las entidades deben **evitar el establecimiento de estructuras complejas y potencialmente no transparentes**, considerando varios aspectos (ej. cumplimiento de las normas internacionales sobre transparencia fiscal, lucha contra el blanqueo de capitales y financiación del terrorismo; en qué medida esa estructura cumple con un propósito económico y legal; etc.). El órgano de dirección debe garantizar la adopción de **medidas de mitigación adecuadas** para evitar los riesgos derivados de actividades en dichas estructuras, lo que incluye que:
  - La entidad cuente con **políticas y procedimientos adecuados** y procesos documentados para la consideración, cumplimiento, aprobación y gestión del riesgo de estas actividades.
  - La información derivada de estas actividades y riesgos sea **accesible** para la entidad, auditores internos y externos, y sea reportada al órgano de dirección en su función supervisora y a la CA.
  - La entidad **revise periódicamente** la necesidad de mantener estas estructuras.

(1) El anexo incluye una lista de los aspectos que deben ser considerados al desarrollar y documentar la política escrita de gobierno interno.

Detalle

Marco de gobierno

Además, las GL establecen que la política de gobierno de la entidad debe ser implementada a nivel de grupo y que las entidades son completamente responsables de todos los servicios externalizados

Marco de gobierno (2/2)

Marco organizativo a nivel de grupo

- La entidad consolidada (a nivel consolidado o sub-consolidado), y las CA deben asegurar que todas las entidades dentro del perímetro de consolidación prudencial, implementen y apliquen una **política de gobierno interno** por escrito que incluya los acuerdos, procesos y mecanismos correspondientes (incluyendo también las filiales no sujetas a la CRD IV y los establecidos en terceros países, incluso en centros financieros extraterritoriales).
- Una entidad consolidada debe considerar los **intereses de todas sus subsidiarias** y cómo las estrategias y políticas contribuyen a largo plazo a los intereses de las subsidiarias y al interés del grupo en su conjunto.

Política de externalización

- El órgano de dirección debe **aprobar y revisar y actualizar regularmente la política de externalización**, considerando el impacto de la externalización sobre el negocio de la entidad y los riesgos a los que está expuesta (ej. operacional, reputacional, riesgo de concentración, etc.). La política debe incluir los mecanismos de reporting y monitorización que deberían implementarse.
- La entidad se mantiene como la **máxima responsable** de todos los servicios y actividades externalizados, así como de las decisiones de gestión adoptadas al respecto.
- Esta política debe establecer que los mecanismos de externalización **no deben obstaculizar la supervisión**, y que no deben contravenir ninguna restricción supervisora sobre los servicios y actividades.

Detalle

Cultura del riesgo y conducta de negocio

Las GL establecen que las entidades deben tener una cultura de riesgos integrada e institucional basada en el riesgo al que están expuestas y que el órgano de dirección debe desarrollar estándares de alto nivel , tanto éticos como profesionales

Cultura del riesgo y conducta de negocio (1/2)

Cultura de riesgos

- Una cultura del riesgo sólida y diligente que debe ser considerada como un **elemento clave de la gestión de riesgos**, y que debe permitir a la entidad tomar decisiones sólidas y fundadas. Así, la entidad debe desarrollar una **cultura de riesgos integrada e institucional** basada, entre otros, en los riesgos a los que está expuesta.
- Los **empleados** deben ser **conscientes de sus responsabilidades** relacionadas con la gestión del riesgo.
- Así, las unidades de negocio bajo supervisión del órgano de dirección son principalmente **responsables de gestionar los riesgo en el día a día**, considerando la capacidad/apetito al riesgo de la entidad.
- Una sólida cultura de riesgos debe incluir las siguientes características: i) '**tone from the top'**, de modo que el órgano de dirección es el responsable de fijar y comunicar los valores/expectativas fundamentales de la entidad, ii) **responsabilidad**, de manera que todos los empleados correspondientes a todos los niveles deben conocer los valores, el apetito y tolerancia al riesgo de la entidad, iii) **comunicación efectiva y challenge**, y iv) **incentivos** para alinear el comportamiento de asunción de riesgos al perfil de riesgo y al interés a largo plazo de la entidad.

Valores y código de conducta

- El **órgano de dirección** debe desarrollar, adoptar, seguir y **promover altos estándares éticos y profesionales**, considerando las necesidades y características específicas de la entidad, con el fin de mejorar los sólidos acuerdos de gobernanza de la institución y reducir los riesgos a los que la entidad está expuesta. A este respecto, las políticas de la institución deben ser neutrales en cuanto al género y evitar cualquier forma de discriminación. El órgano de dirección debe contar con **políticas claras y documentadas** sobre cómo se deben cumplir estos estándares. En concreto, estas políticas deben:
  - Recordar que las actividades deben realizarse cumpliendo las **leyes y los valores corporativos**.
  - Promover la **conciencia del riesgo** a través de una sólida cultura de riesgos.
  - Definir **comportamientos aceptables e inaceptables** (ej. conducta indebida, fraude, blanqueo de capitales, etc.).
  - Aclarar la expectativa de que los empleados deben comportarse con **honestidad** e **integridad**.
  - Garantizar que los empleados son conscientes de las **medidas disciplinarias internas y externas**.

Detalle

Cultura del riesgo y conducta de negocio

Además, las entidades deben contar con una política para identificar, gestionar y mitigar los conflictos de intereses reales y potenciales a nivel institucional y para el personal. Las GL proporcionan guías sobre los procedimientos de alerta interna y la notificación de infracciones

Cultura del riesgo y conducta de negocio (2/2)

Conflictos de interés

- **Política sobre conflictos de interés a nivel institucional**[1]. El órgano de dirección debe establecer, aprobar y supervisar la implementación y la conservación de políticas efectivas para identificar, gestionar y mitigar conflictos de interés actuales y potenciales a nivel institucional. Las medidas de la entidad para gestionar, o si procede, mitigar los conflictos de interés deben documentarse e incluir, entre otros aspectos, una separación de funciones adecuada, límites a la información, etc.).
- **Política sobre conflictos de interés entre el personal**. El órgano de dirección debe mitigar los conflictos reales y potenciales entre los intereses de la entidad y los privados del personal, incluidos los miembros del órgano de dirección, que puedan influir negativamente en el desempeño de sus deberes y responsabilidades.
  - Así, debe establecerse una **política debidamente aprobada** que aborde, entre otros aspectos, ciertas situaciones o relaciones en las que puedan surgir conflictos de interés (ej. intereses económicos, relaciones personales o profesionales, otros empleos, etc.). Esto incluye también la gestión de los conflictos de intereses en el contexto de la concesión de préstamos y la realización de otras transacciones.
  - Esta política debe contar con **procedimientos** (ej. atribuir ciertas actividades u operaciones conflictivas a diferentes personas, impedir influencias inapropiadas, etc.) para prevenir conflictos de interés.

Procedimientos de alerta interna

- Las entidades deben contar con procedimientos para que los **empleados reporten incumplimientos** actuales o potenciales de los **requerimientos regulatorios** (disponibles para todo el personal)[2] y que se cumpla la protección reglamentaria de las personas que denuncian infracciones del Derecho de la Unión.
- A fin de evitar conflictos de interés, la notificación de las infracciones debe llevarse a cabo **fuera del reporting periódico** (ej. a través de la función de cumplimiento, la función de auditoria o un procedimiento interno independiente de denuncia).
- Las entidades deben garantizar la **protección de datos personales** tanto de la persona que reporta el incidente como de la persona que presuntamente es responsable del incumplimiento.

Reporting de incumplimientos a las CA

- Los **procedimientos de alerta interna** deben estar documentados, deben proteger a quien denuncia, garantizar la confidencialidad de la información, etc.
- Las CA deben establecer **mecanismos efectivos** (ej. para conseguir el informe de incumplimientos) que **incentiven a los empleados a reportar a las CA** los incumplimientos de los requerimientos regulatorios actuales o potenciales. También pueden incentivar a los empleados a utilizar, en primera instancia, los procedimientos de alerta interna.

(1) La entidad de consolidación debería considerar los intereses de todas sus filiales.
(2) No debería ser necesario que el empleado tenga prueba de ello, sino un nivel inicial de certidumbre suficiente para iniciar una investigación.

Detalle

Marco de control interno y mecanismos

Las GL orientan sobre el modo en que debe organizarse el marco de control interno y cómo se implementa el control interno

Marco de control interno y mecanismos (1/5)

Marco de control interno

- Las entidades deben desarrollar y mantener una **cultura positiva** hacia el control y el cumplimiento de los riesgos dentro de la entidad y un **marco de control interno robusto y amplio**.
- En este marco, las **líneas de negocio de las entidades** deben ser responsables de la gestión de riesgos que incurren en la realización de sus actividades y deben tener controles que tengan por objeto garantizar el cumplimiento de los requisitos internos y externos.
- El marco de control interno debe adaptarse individualmente a las especificidad de su **negocio**, su c**omplejidad y riesgos asociados**, teniendo en cuenta el contexto del grupo.
- Las instituciones deben aplicar procesos y procedimientos adecuados que garanticen el cumplimiento de sus obligaciones en el contexto de la lucha contra el blanqueo de capitales y la financiación del terrorismo.
- El marco de control interno debe abarcar **toda la organización** incluidas las responsabilidades y tareas del órgano de dirección, así como las actividades de todas las líneas de negocio y unidades internas, incluidas las funciones de control interno, las actividades subcontratadas y los canales de distribución.
- Entre otros aspectos, el **marco de control interno** de una entidad debe garantizar operaciones eficaces y eficientes, una conducta prudente de los negocios, etc.

Implementación del control interno

- El **órgano de dirección** debe ser el responsable de la supervisión y monitorización de la adecuación y efectividad de los procesos y de los mecanismos de control interno, así como de la supervisión de todas las líneas de negocio y unidades internas, incluidas las funciones de control interno [como la gestión del riesgo (including AML/CFT), y las funciones de cumplimiento y auditoria interna].
- Las entidades deben establecer, mantener y **actualizar periódicamente políticas**, mecanismos y procedimientos adecuados de **control interno por escrito** que deben ser aprobados por el órgano de dirección.
- También deben **comunicar esas políticas, mecanismos y procedimientos a todo el personal**, y cada vez que se realicen cambios materiales. Las funciones de control interno deben verificar su implementación.

Detalle

Marco de control interno y mecanismos

Las entidades deben tener un marco de gestión de riesgos en todas las líneas del negocio y funciones de control interno de la entidad. Las GL incluye disposiciones sobre cómo se debe establecer este marco

Marco de control interno y mecanismos (2/5)

Control interno: gestión del riesgo

- Como parte del marco de control interno, las entidades deben tener un **marco holístico de gestión de riesgos** que abarque todas sus **líneas de negocio** y **funciones de control interno**. Este marco debería:
  - Comprender los **riesgos en el balance y fuera de balance** y los **riesgos reales y futuros** a los que puede estar expuesta la entidad (es decir, los riesgos financieros y no financieros[1]).
  - **Evaluar los riesgos** desde una perspectiva **bottom up** y **top down**, dentro y entre las líneas de negocio, utilizando una terminología coherente y metodologías compatibles a nivel consolidado o subconsolidado.
  - Incluir las **políticas**, **procedimientos**, **límites al riesgo** y **controles** que garanticen una adecuada y oportuna identificación, medición, evaluación, monitorización, gestión y reporting de los riesgos a nivel de línea de negocio, entidad y grupo.
  - Proporcionar **directrices específicas** sobre la **implementación de las estrategias** que deben establecer y mantener límites internos en línea con el apetito al riesgo, capital y objetivos estratégicos.
  - Garantizar que en el caso de que se produzca un **incumplimiento de los límites de riesgo**, existe un **proceso para solucionarlo** con un seguimiento adecuado.
  - Estar sujeto a **revisión interna independiente** y ser reevaluado en contra del apetito de riesgo de la entidad, teniendo en cuenta la información del RMF y, donde esté establecido, el comité de riesgo.
  - Desarrollar metodologías apropiadas para la identificación y medición de los riesgos, incluyendo tanto herramientas **forward-looking** (ej. análisis de escenarios y stress test) como **backward-looking** (que consisten en evaluar el perfil de riesgo real y compararlo con el apetito al riesgo).
- Las decisiones que determinan el nivel de riesgos asumidos no solo deben basarse en **información cuantitativa**, sino también emplear un **enfoque cualitativo** (lo que incluye juicio experto y análisis crítico).
- La **responsabilidad última** de la evaluación del riesgo corresponde a la **entidad**, de tal manera que no debe depender exclusivamente de evaluaciones externas (ej. calificaciones de agencias de rating).
- El **reporting de riesgos** efectivo (i.e. bien definidos, documentados y debidamente aprobados por el órgano de dirección) implican una sólida consideración interna y la comunicación de la estrategia de riesgo y los datos de riesgo relevantes (ej. exposiciones e indicadores clave de riesgo).

(1) Incluyendo crédito, mercado, liquidez, concentración, operacional, TI, reputación, legal, conducta, cumplimiento y riesgos estratégicos, AML/CFT y otros delitos financieros y riesgos ESG.

Detalle

Marco de control interno y mecanismos

Estas GL establecen que las entidades deben adoptar una política de aprobación de nuevos productos (NPAP) y que el marco de control interno debe incluir una función de gestión de riesgos, una función de cumplimiento y una función de auditoria interna

Marco de control interno y mecanismos (3/5)

Control interno: nuevos productos

- Se debe contar con una **política de aprobación de nuevos productos (NPAP)** bien documentada, aprobada por el órgano de dirección, que trate el desarrollo de nuevos mercados, productos y servicios, y los cambios significativos sobre los actuales; así como transacciones excepcionales.
- Además se debe contar con **políticas para cambios materiales** sobre los procesos (ej. nuevos mecanismos de externalización) y sobre los sistemas (ej. cambios en los procesos IT).
- En este sentido, la **NPAP** debe: i) **cubrir todas las consideraciones** que deban tenerse en cuenta antes de decidir entrar en nuevos mercados, productos, o servicios, y antes de realizar cambios significativos sobre los existentes; ii) incluir la **definición de 'cambios significativos'** sobre productos/mercados/negocio que deba utilizarse en la organización, así como las funciones internas que están involucradas en la toma de decisiones; y iii) exponer los **principales problemas** que deben tratarse antes de tomar una decisión (ej. cumplimiento de regulación, contabilidad, modelos de pricing, impactos en el perfil de riesgo, etc.). iv) identificar y evaluar el riesgo de BC/FT asociado al nuevo producto o práctica comercial, y establecer las medidas a tomar para mitigar dichos riesgos.
- La **RMF** debe estar también involucrada en la **aprobación de nuevos productos** o **cambios significativos** a los ya existentes y debe tener una visión general del **roll-out de nuevos productos**.

Control interno: funciones

- Las funciones de control interno deben incluir una **funciones de gestión de riesgos**, **de cumplimiento** y **de auditoría interna** [1]. La función de gestión de riesgos y la función de cumplimiento pueden combinarse, mientras que la función de auditoría interna no debe combinarse con ninguna otra función de control.

Responsables de las funciones de control interno

- Los responsables de las funciones de control interno deben designarse según un nivel jerárquico adecuado con autoridad y categoría apropiadas para cumplir con sus responsabilidades. Deben ser **independientes** de las líneas de negocio que gestionan, y deben reportar directamente al órgano de dirección.
- A fin de garantizar su independencia, deben seguir varias condiciones (ej. su personal no debe realizar las tareas operacionales que deben supervisar, organizarlas por separado, etc.)

Recursos de las funciones de control interno

- Las funciones de control interno deben contar con **suficientes recursos.** Deben tener un número adecuado de empleado cualificados (a nivel matriz y filial) y deben ser cualificados de forma continua y recibir formación cuando sea necesario.

(1) Incluyendo el cumplimiento de los requisitos ALD/CTF. Las entidades pueden establecer una función separada de cumplimiento de PBC/FT como una función de control independiente

Detalle

Marco de control interno y mecanismos

Las entidades deben contar con un marco de gestión del riesgo para todas las líneas de negocio y funciones de control interno. Las GL establecen directrices sobre cómo debería establecerse dicho marco…

Marco de control interno y mecanismos (4/5)

Función de control interno: RMF

- Las entidades deben establecer una RMF con **suficiente autoridad y recursos** para implementar las políticas de riesgo y el marco de gestión del riesgo.
- Consecuentemente, debería ser una **función central de la entidad**[1], y debería tener **acceso directo** al órgano de dirección en su función de supervisión y a los comités, a todas las líneas de negocio y otras unidades internas con potencial para generar riesgos, así como a las filiales relevantes.
- Los empleados de la RMF deben tener **conocimientos, habilidades y experiencia suficiente** sobre técnicas de gestión del riesgo, mercados y productos; y deben tener acceso a formación periódica.
- La RMF debería ser **independiente de las líneas y unidades de negocio cuyos riesgos controla**, aunque no se le debería prohibir interactuar con ellas.
- La RMF debería proporcionar **información relevante e independiente**, análisis y juicio experto sobre exposiciones de riesgo, así como asesoramiento sobre las propuestas y decisiones de riesgo planteadas por las líneas de negocio o unidades internas, o por el órgano de dirección, en relación a si dichas propuestas son consistentes con el apetito al riesgo y la estrategia de riesgo de la entidad.
- La RMF podría recomendar **mejoras** sobre el marco de gestión del riesgo, así como **medidas correctivas** para solventar incumplimientos en las políticas, procedimientos y límites de riesgos.
- En relación al **rol de la RMF**, ésta debe involucrarse activamente en, entre otros, la estrategia de riesgo (ej. la RMF debe proporcionar al organismo de gestión toda la información relevante relacionada con el riesgo para establecer el nivel de apetito del riesgo de la entidad, evaluar la solidez y sostenibilidad de la estrategia de riesgo y apetito, etc.); en los cambios materiales, identificación, medición, evaluación, gestión, monitorización y reporting de los riesgos; y exposiciones no aprobadas.
- El **responsable de la RMF** debería proporcionar información global y comprensible sobre riesgos. En el caso de que no esté justificado nombrar a una persona dedicada solo a este cargo, puede realizarse **conjuntamente con la función de cumplimiento** o puede realizarse por otra persona (sin conflicto de interés).

(1) Las entidades sistémicas podrían considerar establecer una RMF para cada línea de negocio material. No obstante, debería existir una RMF central, incluyendo una RMF en la entidad consolidada a nivel grupo.

Detalle

Marco de control interno y mecanismos

…así como una función de cumplimiento para gestionar el riesgo de cumplimiento de la entidad, y una función de auditoría interna (IAF) que debería evaluar, entre otros aspectos, la calidad del marco de control interno

Marco de control interno y mecanismos (5/5)

Función de control interno: cumplimiento

- La entidad debe establecer una función de cumplimento permanente y efectiva para gestionar su **riesgo de cumplimiento**[1], y nombrar una persona responsable de esta función en la entidad (‘Compliance Officer’ o responsable de cumplimiento).
- La **función de cumplimiento** debe ser independiente de las líneas de negocio y de las unidades internas bajo su control, y debe contar con suficiente autoridad y recursos.
- Los empleados de la función de cumplimiento deben tener **conocimientos, habilidades y experiencia suficiente** sobre cumplimiento, y deben tener acceso a formación periódica.
- El órgano de dirección en su función de supervisión, debe **controlar la implementación** de una política de cumplimiento bien documentada, que debe comunicarse a todo el personal.
- Además, debe **asesorar al órgano de dirección** sobre las leyes, normas y estándares que las entidades tienen que cumplir, así como evaluar el posible impacto de los cambios en el marco regulatorio.

Función de control interno: auditoría interna

- La entidad debe establecer una **función de auditoría interna independiente**, considerando el criterio de proporcionalidad, y nombrar una persona responsable de esta función en toda la entidad. En este sentido, la IAF debe:
  - Ser **independiente** y tener suficiente autoridad y recursos.
  - Realizar una **revisión independiente** sobre el cumplimiento de todas las actividades y unidades de la entidad.
  - Evaluar la **calidad del marco de control interno** considerando, entre otros, la idoneidad de dicho marco, si las políticas y procedimientos son adecuados y cumplen con los requerimientos legales, con el apetito al riesgo y la estrategia, etc.
- El **responsable de la IAF** debe ser capaz de reportar directamente y por iniciativa propia al órgano de dirección en su función de supervisión la no-implementación de las medidas correctivas propuestas.
- La función de auditoría interna debe realizarse de acuerdo con el **plan de auditoría**, el cual debe elaborarse **al menos anualmente** conforme a los objetivos de control anuales.

(1) Las entidades deben tomar las medidas adecuadas contra los comportamientos internos o externos que puedan facilitar o permitir el fraude, el blanqueo de capitales y el financiamiento de otros delitos financieros y el incumplimiento de la disciplina.

Detalle

Gestión de continuidad de negocio

Las entidades deben contar con una sólida gestión de continuidad del negocio para reducir las consecuencias derivadas de un fallo o una interrupción extendida sobre recursos críticos

Gestión de continuidad de negocio

Gestión de continuidad de negocio

- Las entidades deben establecer una sólida gestión de continuidad del negocio para reducir las **consecuencias operacionales, financieras, legales, reputacionales** y **de otras materias** derivadas de un fallo o una interrupción extendida.
- Deben analizar su exposición a graves **interrupciones del negocio** y evaluar (cuantitativamente y cualitativamente) su **impacto potencial**, usando datos externos e internos y un análisis de escenarios.
- Sobre la base de dicho análisis, las entidades deben poner en marcha **planes de continuidad del negocio y de contingencia**, así como **planes de recuperación**, que deben estar documentados.
- Además, una función de continuidad del negocio operativo (la '**Función de Gestión del Riesgo Operacional**'), parte de la RMF, debe estar involucrada activamente para aquellas entidades que usan AMA[1].

(1) Advanced Measurement Approaches (AMA)

Detalle

Principios aplicados al marco de gobierno interno

La EBA especifica que las entidades deben aplicar los principios de proporcionalidad y transparencia para establecer mecanismos de gobierno interno alineados con el perfil de riesgo y el modelo de negocio de la entidad y para que los empleados estén informados

Principios aplicados al marco de gobierno interno

Proporcionalidad

- Las entidades deben considerar su **tamaño**, **organización interna** y la **naturaleza** y **complejidad** de sus actividades a la hora de desarrollar e implementar mecanismos de gobierno interno.
- Entre otros, las **entidades** y **CAs deben considerar** la presencia geográfica de la entidad y el volumen de las operaciones en cada jurisdicción, la forma legal, si la entidad es parte de un grupo, etc.
- De acuerdo con el principio de proporcionalidad:
  - Las entidades sistémicas y las entidades y grupos más complejos deben tener **mecanismos de gobierno más sofisticados**.
  - Las entidades y grupos menores no complejos pueden implementar **mecanismos de gobierno más sencillos**.

Transparencia

- El órgano de dirección debe **informar a los empleados** sobre las estrategias y políticas de la entidad de manera clara y consistente, al menos al nivel necesario para llevar a cabo sus tareas particulares (ej. mediante políticas escritas, manuales, etc.).
- Cuando la matriz esté requerida por la CA a publicar anualmente una descripción de su estructura legal y de gobierno y de la estructura organizativa del grupo de entidades, la información debe incluir a **todas las entidades** que se encuentran **dentro de la estructura de grupo** y debe presentarse por país.
- La **publicación debe incluir**, entre otros:
  - Un resumen de la **organización interna** de la entidad y de la estructura de grupo, incluyendo las principales líneas de reporting y las responsabilidades.
  - Cualquier **cambio material**, en comparación con la publicación anterior.
  - **Nuevas estructuras** legales, de gobierno u organizativas.
  - Una visión general de la **externalización material** de actividades, procesos y sistemas.
  - Información sobre la estructura, organización, responsabilidades y miembros del **órgano de dirección**.
  - Una lista de los **comités del órgano de dirección** en su función supervisora y su composición.

Índice

Próximos pasos

Estas GL finales sobre gobierno interno se aplicarán a partir del 30 de junio de 2018. En consecuencia, las Directrices actuales sobre gobierno interno (GL 44) quedarán derogadas en esa misma fecha

Próximos pasos

- Estas GL se aplicarán a las autoridades competentes de la UE, y a las entidades tanto a nivel individual como consolidado, a partir del **31 de diciembre de 2021**.
- Las Directrices existentes sobre gobernanza interna (GL 2017) serán derogadas en la misma fecha.

Índice

Anexo
Política de gobierno interno

Las entidades deben considerar cierto aspectos (ej. estructura de accionistas, estructura de grupo, etc.) a la hora de desarrollar y documentar la política de gobierno interno

Política de gobierno interno (documento escrito)

1. Estructura de accionistas
2. Estructura de grupo, (estructura legal y funcional, si aplica)
3. Composición y funcionamiento del órgano de dirección
a) criterios de selección incluida la forma en que se tiene en cuenta la diversidad b) número, duración del mandato, rotación, edad c) miembros independientes del órgano de dirección d) miembros ejecutivos del órgano de dirección e) miembros no ejecutivos del órgano de dirección f) división interna de tareas, si aplica
4. Estructura de gobierno y organigrama (con impacto sobre el grupo, si aplica)
a) comités especializados i. composición ii. funcionamiento
b) comité de gestión, si existe i. composición ii. funcionamiento (regulación interna)
5. Titulares de funciones clave
a) Responsable de la función de gestión de riesgo b) Responsable de la función de cumplimiento c) Responsable de la función de auditoría d) Chief Financial Officer (CFO) e) Otros titulares de funciones clave

6. Marco de control interno
a) descripción de cada función (recursos, categoría, autoridad) b) descripción del marco de gestión de riesgo incluyendo estrategia de riesgo
7. Estructura organizativa (con impacto sobre grupo, si aplica)
a) estructura operacional, líneas de negocio y asignación de competencias y responsabilidades b) externalización c) rango de productos y servicios d) ámbito geográfico del negocio e) prestación libre de servicios f) sucursales g) filiales, joint ventures, ... h) uso de centros off-shore
8. Código de conducta y comportamiento (con impacto sobre grupo, si aplica)
a) objetivos estratégicos y valores empresariales b) códigos internos y reglamentos, política de prevención c) política de conflictos de interés d) denuncias
9. Status de la política interna (detallando la fecha correspondiente)
a) desarrollo b) última modificación c) última evaluación d) aprobación por el órgano de dirección