teasa Consulting

ESTRATEGIA | ORGANIZACIÓN | MANAGEMENT

Gestión de Riesgos

CONTROL Y COMPLIANCE

¿Qué entendemos por Compliance?

Es el **Sistema que implementan las sociedades para asegurar** no sólo el cumplimiento de las disposiciones legales y normativas que le aplican, sino también el **cumplimiento de las normas internas éticas y de comportamiento de los miembros de la Organización.**

La función de Compliance abarca tres ámbitos:

- **Governance:** conjunto de mecanismos para asegurar un Modelo de Gobierno que garanticen que las decisiones se toman con total información y que se establecen los controles adecuados para confirmar que las instrucciones y la estrategia se están desarrollando correctamente.
- **Gestión de Riesgos.**
- **Compliance:** se encarga no sólo del cumplimiento de las regulaciones y leyes que resulten aplicables, sino también de la redacción y aprobación de las políticas, compromisos y valores internos y de las funciones de control y supervisión.

¿Y por gestión de riesgos?

La **Gestión de Riesgos** es el proceso de identificación, análisis y evaluación de cualquier actuación, hechos o proceso (riesgo) que pueda **afectar de forma adversa a la estrategia de la organización**, su capacidad de operar y el cumplimiento de los objetivos económicos o reputacionales, ya sean **riesgos corporativos o penales.**

La gestión de estos riesgos **se puede realizar a través de su mitigación** (reducir impacto o probabilidad), **prevención** (evitar el riesgo), **aceptación** según apetito al riesgo, **o compartirlos**, por ejemplo póliza de seguros.

¿Por qué lo necesito?

- **Se aplica a todas las empresas independientemente del sector y tamaño,** si bien se especifica que el Sistema se adecuará precisamente a estas circunstancias

- **Son requerimientos que cada vez están más exigiendo las compañías** para operar comercialmente con Terceros, ya sea como proveedor o clientes.

- **Su correcta implementación comporta exenciones o reducciones de la responsabilidad penal de la persona jurídica y de los administradores y directivos,** así como reducción o eliminación de sanciones económicas y administrativas.

- **Se valora mucho en el Mercado junto con los criterios ESG** (Medio Ambiente, Social y Personas), **Governance** (Compliance) **y refuerza la Compañía.**

¿Cómo lo haremos?

Utilizamos metodología contrastada siguiendo las directrices establecidas en diferentes Normas ISO y UNE de aplicación ISO 37001 Gestión de Riesgos, ISO 37301 Sistema de Gestión de Compliance, UNE 19601 Sistema de Gestión de Compliance Penal.

Ejemplos de necesaria aplicación:

- **¿Qué tipo de controles tiene establecidos** una empresa de reciclaje para **controlar las compras de materias primas (por ejemplo cobre)?**
- **¿Cómo gestiona una empresa la identificación, análisis y valoración de la integridad de los Terceros** con los que mantenemos o queremos iniciar relaciones comerciales?
- ¿La compañía tiene implementadas **medidas o políticas anticorrupción y contra el fraude?**
- ¿La empresa dispone de **políticas en el área de RRHH contra el acoso, plan de igualdad en su caso?**
- ¿La Pyme tiene actualizado el **canal de denuncia según la L2/2023?**

01 Punto de partida de la empresa

01 Punto de partida de la empresa

Posibles escenarios en los que se puede encontrar su empresa u organización:

- La empresa NO tiene implementado un **Sistema de Gestión de Riesgos**.
- No existen responsabilidades asignadas en cuestiones **de riesgos, ni en las funciones de control y supervisión.**
- **Han trabajado los riesgos y controles, pero disponen de un mapa de riesgos no actualizado:** NO hacen seguimiento.
- **Si tienen un Sistema de Gestión de Riesgos:** Se necesitaría una Auditoría y una revisión del Modelo.

02 Objetivos

02 Objetivos

El proyecto persigue alzanzar cuatro objetivos:

- **Identificar los riesgos inherentes y residuales:** análisis, valoración y evaluación.
- **Análisis, eficacia y eficiencia de los controles:** valoración del sistema de control interno.
- **Elaborar el Mapa de Riesgos:** corporativo y penal.
- **Establecer planes de revisión y mejora en la gestión de riesgos:** implementar controles.

03 Desarrollo del Proyecto

03 Desarrollo del Proyecto

El proyecto se desarrolla en 5 fases y en 4 formatos de trabajo diferentes:

Fase 1
Contrastar cultura de cumplimiento y consensuar metodología

Fase 2
Identificación y categorización de los riesgos inherentes

Fase 3
Análisis de la eficacia y eficiencia de los controles

Fase 4
Mapa de riesgos corporativo y penal

Fase 5
Planes de acción y de mejora


Sesión presencial


Sesión digital


Trabajo interno empresa


Trabajo consultor

03 Desarrollo del Proyecto

Fase 1 Contrastar cultura de cumplimiento y consensuar metodología

Fase 2 Identificación y categorización de los riesgos inherentes

Fase 3 Análisis de la eficacia y eficiencia de los controles

Fase 4 Mapa de riesgos corporativo y penal

Fase 5 Planes de acción y de mejora

Objetivo

Contrastar la cultura de cumplimiento y el modelo de gestión de riesgos.
Consensuar metodología y formados por la elaboración del mapa de riesgos corporativo y penal.

Acciones

- Reunión con la Administración para contrastar la cultura de cumplimiento, la tolerancia al riesgo y el sistema de gestión de riesgos.
- Planteamiento de diversos aspectos clave para la elaboración del Mapa de Riesgos:
  - ✓ Metodología para la Identificación y Desarrollo de las entrevistas con los responsables.
  - ✓ Apoyo electrónico para la recogida de información.
  - ✓ Selección de áreas y ámbitos para identificar los riesgos penales y los riesgos claves corporativos.
  - ✓ Calendario de actuación y comunicación.

Resultado/Entregables

Formato y enfoque consensuado del Mapa de Riesgos.
Formato Excel por la recogida y administración de la información durante el proyecto.

03 Desarrollo del Proyecto

Fase 1	**Fase 2**	Fase 3	Fase 4	Fase 5
Contrastar cultura de cumplimiento y consensuar metodología	Identificación y categorización de los riesgos inherentes	Análisis de la eficacia y eficiencia de los controles	Mapa de riesgos corporativo y penal	Planes de acción y de mejora

Objetivo

Identificación, análisis y evaluación de los riesgos propios de la actividad de la Organización por su valoración.

Acciones

- En cada una de las áreas y funciones seleccionadas, teasa realizará un trabajo previo donde identificará los siguientes aspectos:
  - ✓ Clasificación y categorización según impacto y probabilidad.
  - ✓ Relación de los riesgos más relevantes por cada uno de los procesos desarrollados por el área o función.
  - ✓ De los riesgos categorizados como clave, identificación de los potenciales delitos.
- Determinar los riesgos por área responsable o ámbito, así como impacto y responsabilidad con los distintos responsables.

Resultado/Entregables

Excel de riesgo del área/función con riesgos identificados, categorizados.
Acerca de los Claves, delitos potenciales, y elementos a controlar.

03 Desarrollo del Proyecto

Fase 1	Fase 2	Fase 3	Fase 4	Fase 5
Contrastar cultura de cumplimiento y consensuar metodología	Identificación y categorización de los riesgos inherentes	Análisis de la eficacia y eficiencia de los controles	Mapa de riesgos corporativo y penal	Planes de acción y de mejora

Objetivo

Identificación, análisis y evaluación de los riesgos propios de la actividad de la Organización por su valoración.

Acciones

- teasa desarrollará en trabajo interno la Fase 2 y remitirá a los Excels con los resultados. Toda la actividad según calendario Fase 1.
- Determinados los riesgos inherentes, en esta fase se analizarán eficacia y eficiencia de los controles:
  - ✓ Clasificación y categorización según impacto y probabilidad del riesgo residual.
  - ✓ Relación y evaluación de los controles.
- Determinar los riesgos por área responsable o ámbito, así como impacto y responsabilidad con los distintos responsables.
- Estas reuniones tratarán de ser muy ejecutivas (por eso enviamos la información previa).

Resultado/Entregables

Excel con detalle de los controles actuales por cada riesgo y evaluación del residual según impacto y probabilidad.

03 Desarrollo del Proyecto

teasaConsulting
ESTRATEGIA | ORGANIZACIÓN | MANAGEMENT

Fase 1 Contrastar cultura de cumplimiento y consensuar metodología

Fase 2 Identificación y categorización de los riesgos inherentes

Fase 3 Análisis de la eficacia y eficiencia de los controles

Fase 4 Mapa de riesgos corporativo y penal

Fase 5 Planes de acción y de mejora

Objetivo

Elaborar Mapa de riesgos penales y corporativos.

Acciones

Descripción del riesgo	Categ. del riesgo	Tipología del riesgo	Impacto	Probabilidad	Resultado riesgo inherente	Control/ Medidas preventivas actuales	Impacto tras control	Probabilidad tras control	Resultado riesgo residual (RR)	Nivel de riesgo residual	Área/Posición Responsable	Riesgo aceptable
Falta de política de seguridad IT (no documentada)	Operativos	Tecnología	4. Alto	3. Ocasional	12	Están elaborando Política. Se aprueba por el responsable del Departamento. El Director de Área decide los accesos	4. Alto	2. Posible	8		Departamento de Sistemas	
Falta de Política de uso de medios tecnológicos documentada (claves acceso, dispositivos, uso personal,...)	Operativos	Tecnología	4. Alto	4. Alta	16		4. Alto	3. Ocasional	12		Departamento de Sistemas	
Ciberataque externo o "secuestro" de información/sistemas	Operativos	Tecnología	5. Crítico	5. Muy alta	25	Firewalls de acceso, acceso red nominativos, todo securizado	5. Crítico	3. Ocasional	15		Departamento de Sistemas	
Incumplimiento de la Ley de Protección Datos Personales	Operativos	Tecnología	4. Alto	2. Posible	8	CPD independientes para garantizar la seguridad de la información y evitar que ataques externos afectes la	3. Moderado	1. Poco probable	3		Departamento de Sistemas	Sí
Pérdida de datos o información asociada a sistemas. Seguridad de la información.	Operativos	Tecnología	5. Crítico	5. Muy alta	25		3. Moderado	1. Poco probable			Departamento de	Sí

Impacto		
	Crítico	5
	Alto	4
	Moderado	3
	Menor	2
	Insignificante	1

5	10	15	20	25
4	8	12	16	20
3	6	9	12	15
2	4	6	8	10
1	2	3	4	5

Probabilidad				
Poca	Posible	Ocasional	Alta	Muy alta
1	2	3	4	5

Resultado/Entregables

Excel con Mapa de riesgos corporativos y Mapa de color de riesgos penales.

03 Desarrollo del Proyecto

teasa Consulting
ESTRATEGIA | ORGANIZACIÓN | MANAGEMENT

Fase 1	Fase 2	Fase 3	Fase 4	Fase 5
Contrastar cultura de cumplimiento y consensuar metodología	Identificación y categorización de los riesgos inherentes	Análisis de la eficacia y eficiencia de los controles	Mapa de riesgos corporativo y penal	Planes de acción y de mejora

Objetivo

Presentación del Mapa de Riesgos penales y corporativos y los planes de acción y mejora en la gestión de los riesgos.

Acciones

Plan de acción Mecanismo control adicional	Responsable	Fecha máxima realización	Estado situación

Resultado/Entregables

Mapa de riesgos penal (mapa de color) y los riesgos corporativos (Excel) con los Planes de acción y mejora.

Gracias

teasa

C/ Sardenya, 397-399 2n 5a
08025 Barcelona
Tel. 934 874 260
Email: teasa@teasa.es
www.teasa.es

teasa Consulting

ESTRATEGIA | ORGANIZACIÓN | MANAGEMENT

teasatech

TRANSFORMACIÓN DIGITAL | INDUSTRIA 4.0 | INNOVACIÓN