teasa Consulting

ESTRATÈGIA | ORGANITZACIÓ | MANAGEMENT

Gestió de Riscos

CONTROL I COMPLIANCE

Què entenem per Compliance?

És el **Sistema que implementen les societats per assegurar** no únicament el compliment de les disposicions legals i normatives que li apliquen, sinó també el **compliment de les normes internes ètiques i de comportament dels membres de l'Organització.**

La funció de Compliance abasta tres àmbits:

- **Governance:** conjunt de mecanismes per assegurar un Model de Govern que garanteixin que les decisions es prenen amb total informació i que s'estableixen els controls adients per confirmar que les instruccions i l'estratègia s'estan desenvolupant correctament.
- **Gestió de Riscos.**
- **Compliance:** s'encarrega no només del compliment de les regulacions i les Lleis que resultin aplicables, sinó també de la redacció i aprovació de les polítiques, compromisos i valors interns i de les funcions de control i supervisió.

I per gestió de riscos?

La **Gestió de Riscos** és el procés d'identificació, anàlisi i avaluació de qualsevol actuació, fets o procés (risc) que pugui **afectar de forma adversa l'estratègia de l'organització**, la seva capacitat d'operar i el compliment dels objectius econòmics o reputacionals, ja siguin **riscos corporatius o penals.**

La gestió d'aquests riscos **es pot realitzar a través de la seva mitigació** (reduir impacte o probabilitat), **prevenció** (evitar el risc), **acceptació** segons "apetito al riesgo", **o compartir-los**, per exemple pòlissa d'assegurances.

Per què ho necessito?

- **Aplica a totes les empreses independentment del sector i dimensió**, si bé s'especifica que el Sistema s'adequarà precisament a aquestes circumstàncies.
- **Son requeriments que cada vegada més estan exigint les companyies** per operar comercialment amb Tercers, ja sigui com a proveïdor o clients.
- **La seva correcta implementació comporta exempcions o reduccions de la responsabilitat penal de la persona jurídica i dels administradors i directius**, així com reducció o eliminació de sancions econòmiques i administratives.
- **Es valora molt en el Mercat juntament amb els criteris ESG** (Medi Ambient, Social i Persones), **Governance** (Compliance) **i reforça la Companyia.**

Com ho farem?

Utilitzem metodologia contrastada seguint les directrius establertes en diferents Normes ISO i UNE d'aplicació ISO 37001 Gestión de Riesgos, ISO 37.301 Sistema de Gestión de Compliance, UNE 19601 Sistema de Gestión de Compliance Penal.

Exemples de necessària aplicació:

- **Quin tipus de controls té establerts** una empresa de reciclatge per **controlar les compres de primeres matèries (per exemple coure)?**
- **Com gestiona una empresa l'identificació, anàlisi i valoració de la integritat dels Tercers** amb els què mantenim o volem iniciar relacions comercials?
- La companyia té implementades **mesures o polítiques anticorrupció i contra el frau?**
- L'empresa disposa de **polítiques en l'àrea de RRHH contra l'assetjament, pla d'igualtat si s'escau?**
- La Pime té actualitzat el **canal de denúncia segons la L2/2023?**

01 Punt de partida de l'empresa

01 Punt de partida de l'empresa

Possibles escenaris on es pot trobar la seva empresa o organització:

- La empresa NO té implementat un **Sistema de Gestió de Riscos**.
- No hi ha responsabilitats assignades en qüestions **de riscos, ni en les funcions de control i supervisió.**
- **Han treballat els riscos i els controls, però disposen d' un mapa de riscos no actualitzat:** NO fan seguiment.
- **Si que tenen un Sistema de Gestió de Riscos:** Caldría una Auditoria i una revisió del Model.

02 Objectius

02 Objectius

El projecte persegueix assolir quatre objectius:

- **Identificar els riscos inherents i residuals:** anàlisi, valoració i avaluació.
- **Anàlisi, eficàcia i eficiència dels controls:** valoració del sistema de control intern.
- **Elaborar el Mapa de Riscos:** corporatiu i penal.
- **Establir plans de revisió i millora en la Gestió de Riscos:** implementar controls.

03 Desenvolupament del Projecte

03 Desenvolupament del Projecte

El projecte es desenvolupa en 5 fases i en 4 formats de treball diferents:

Fase 1
Contrastar cultura de compliment i consensuar metodologia

Fase 2
Identificació i categorització dels riscos inherents

Fase 3
Anàlisi de la eficàcia i eficiència dels controls

Fase 4
Mapa de riscos corporatiu i penal

Fase 5
Plans d' acció i de millora


Sessió presencial


Sessió digital


Treball intern empresa


Treball consultor

03 Desenvolupament del Projecte

Fase 1 Contrastar cultura de compliment i consensuar metodologia

Fase 2 Identificació i categorització dels riscos inherents

Fase 3 Anàlisi de la eficàcia i eficiència dels controls

Fase 4 Mapa de riscos corporatiu i penal

Fase 5 Plans d' acció i de millora

Objectiu

Contrastar la cultura de compliment i el model de gestió dels riscos.
Consensuar metodologia i formats per la elaboració del mapa de riscos corporatiu i penal.

Accions

- Reunió amb l'Administració per contrastar la cultura de compliment, la tolerància al risc i el sistema de gestió de riscos.
- Plantejament de diversos aspectes clau per l'elaboració del Mapa de Riscos:
  - ✓ Metodologia per l'Identificació i Desenvolupament de les entrevistes amb els responsables.
  - ✓ Support electrònic per la recollida d' informació.
  - ✓ Selecció d'àrees i àmbits per identificar els Riscos Penals i els Riscos Claus Corporatius.
  - ✓ Calendari d'actuació i comunicació.

Resultat/Lliurables

Format i enfoc consensuat del Mapa de Riscos.
Format Excel per la recollida i administració de l'informació durant el projecte.

03 Desenvolupament del Projecte

Fase 1	**Fase 2**	Fase 3	Fase 4	Fase 5
Contrastar cultura de compliment i consensuar metodologia	Identificació i categorització dels riscos inherents	Anàlisi de la eficàcia i eficiència dels controls	Mapa de riscos corporatiu i penal	Plans d' acció i de millora

Objectiu	Identificació, anàlisi i avaluació dels riscos propis de l'activitat de l'Organització per la seva valoració.

Accions

- En cada una de les àrees i funcions seleccionades, teasa farà un treball previ on identificarà els següents aspectes:
  - ✓ Classificació i categorització segons impacte i probabilitat.
  - ✓ Relació dels riscos més rellevants per cada un dels processos desenvolupats per l'àrea o funció.
  - ✓ Dels riscos categoritzats com a Clau, identificació dels potencials delictes.
- Determinar els riscos per àrea responsable o àmbit, així com impacte i responsabilitat amb els diferents responsables.

Resultat/Lliurables	Excel de risc de l'àrea/funció amb riscos identificats, categoritzats. Sobre els Claus, delictes potencials, i elements a controlar.

03 Desenvolupament del Projecte

Fase 1	Fase 2	Fase 3	Fase 4	Fase 5
Contrastar cultura de compliment i consensuar metodologia	Identificació i categorització dels riscos inherents	Anàlisi de la eficàcia i eficiència dels controls	Mapa de riscos corporatiu i penal	Plans d' acció i de millora

Objectiu

Identificació, anàlisi i avaluació dels riscos propis de l'activitat de l'Organització per la seva valoració.

Accions

- teasa desenvoluparà en treball intern la Fase 2 i remetrà els Excels amb els resultats. Tota l' activitat segons calendari Fase 1.
- Determinats els riscos inherents, en aquesta fase s'analitzaran eficàcia i eficiència dels controls:
  - ✓ Classificació i categorització segons impacte i probabilidad del risc residual.
  - ✓ Relació i avaluació dels controls.
- Determinar els riscos per àrea responsable o àmbit, així com impacte i responsabilitat amb els diferents responsables.
- Aquestes reunions tractaran de ser molt executives (per això enviem la informació prèvia).

Resultat/Lliurables

Excel amb detall dels controls actuals per cada risc i avaluació del residual segons impacte i probabilitat.

03 Desenvolupament del Projecte

Fase 1 Contrastar cultura de compliment i consensuar metodologia

Fase 2 Identificació i categorització dels riscos inherents

Fase 3 Anàlisi de la eficàcia i eficiència dels controls

Fase 4 Mapa de riscos corporatiu i penal

Fase 5 Plans d' acció i de millora

Objectiu

Elaborar Mapa de riscos penals i corporatiu.

Accions

Descripción del riesgo	Categ. del riesgo	Tipología del riesgo	¿Aspecto delictivo?	¿En qué delito impacta?	Impacto	Probabilidad	Resultado riesgo inherente	Control/ Medidas preventivas actuales	Impacto tras controles	Probabilidad tras control	Resultado riesgo residual (1-25)	Nivel de riesgo residual	Área/Posición Responsable	Riesgo aceptable
Falta de política de seguridad IT (no documentada)	Operativos	Tecnológica	NO		4. Alto	3. Ocasional	12	Está 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	Tecnológica	No		4. Alto	4. Alto	16		4. Alto	3. Ocasional	12		Departamento de Sistemas	
Ciberataque externo o "secuestro" de información/sistemas	Operativos	Tecnológica	SÍ	Delito Tecnológico	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	Tecnológica	SÍ	Delito contra la intimidad y/o por revelacion datos	4. Alto	2. Posible	8	CPD independiente para garantizar la seguridad de la información y evitar que ataques externos afecten la	3. Moderado	1. Poco probable	3		Departamento de Sistemas	SÍ
Pérdida de datos o información asociada a sistemas. Seguridad de la información.	Operativos	Tecnológica	SÍ	Delito Tecnológico	5. Crítico	5. Muy alta	25		3. Moderado	1. Poco probable			Departamento de	SÍ

Impacte		
	Crític	5
	Alt	4
	Moderat	3
	Menor	2
	Insignificant	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

Probabilitat				
Poc probable	Posible	Ocasional	Alta	Molt alta
1	2	3	4	5

Resultat/Lliurables

Excel amb Mapa de riscos corporatius i Mapa de color dels riscos penals.

03 Desenvolupament del Projecte

Fase 1	Fase 2	Fase 3	Fase 4	Fase 5
Contrastar cultura de compliment i consensuar metodologia	Identificació i categorització dels riscos inherents	Anàlisi de la eficàcia i eficiència dels controls	Mapa de riscos corporatiu i penal	Plans d' acció i de millora

Objectiu

Presentació del Mapa de Riscos penals i corporatiu i els plans d'acció i de millora en la gestió dels riscos.

Accions

Pla d'acció Mecanisme control addicional	Responsable	Data màxima realització	Estat situació

Resultat/Lliurables

Mapa de riscos penal (mapa de color) i els riscos corporatius (Excel) amb els Plans d'acció i millora.

Gràcies

teasa

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

teasa Consulting

ESTRATÈGIA | ORGANITZACIÓ | MANAGEMENT

teasatech

TRANSFORMACIÓ DIGITAL | INDÚSTRIA 4.0 | INNOVACIÓ