

teasaConsulting
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**:

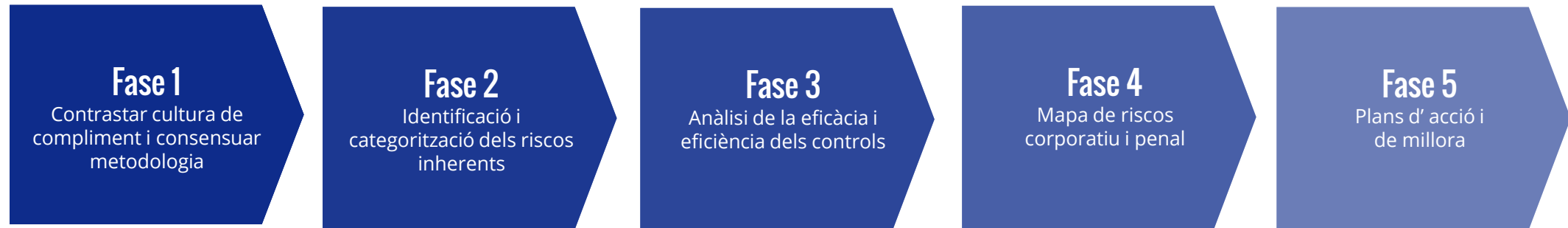
- **Identificar els riscos inherents i residuals:** anàlisi, valoració i avaluació.
- **Anàlisi, eficàcia i eficiència dels controls:** valoració del sistema de control intern.
- **Elaborar el Mapa de Riscos:** corporatiu i penal.
- **Establir plans de revisió i millora en la Gestió de Riscos:** implementar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



03 Desenvolupament del Projecte

03 Desenvolupament del Projecte

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



Sessió presencial



Sessió digital

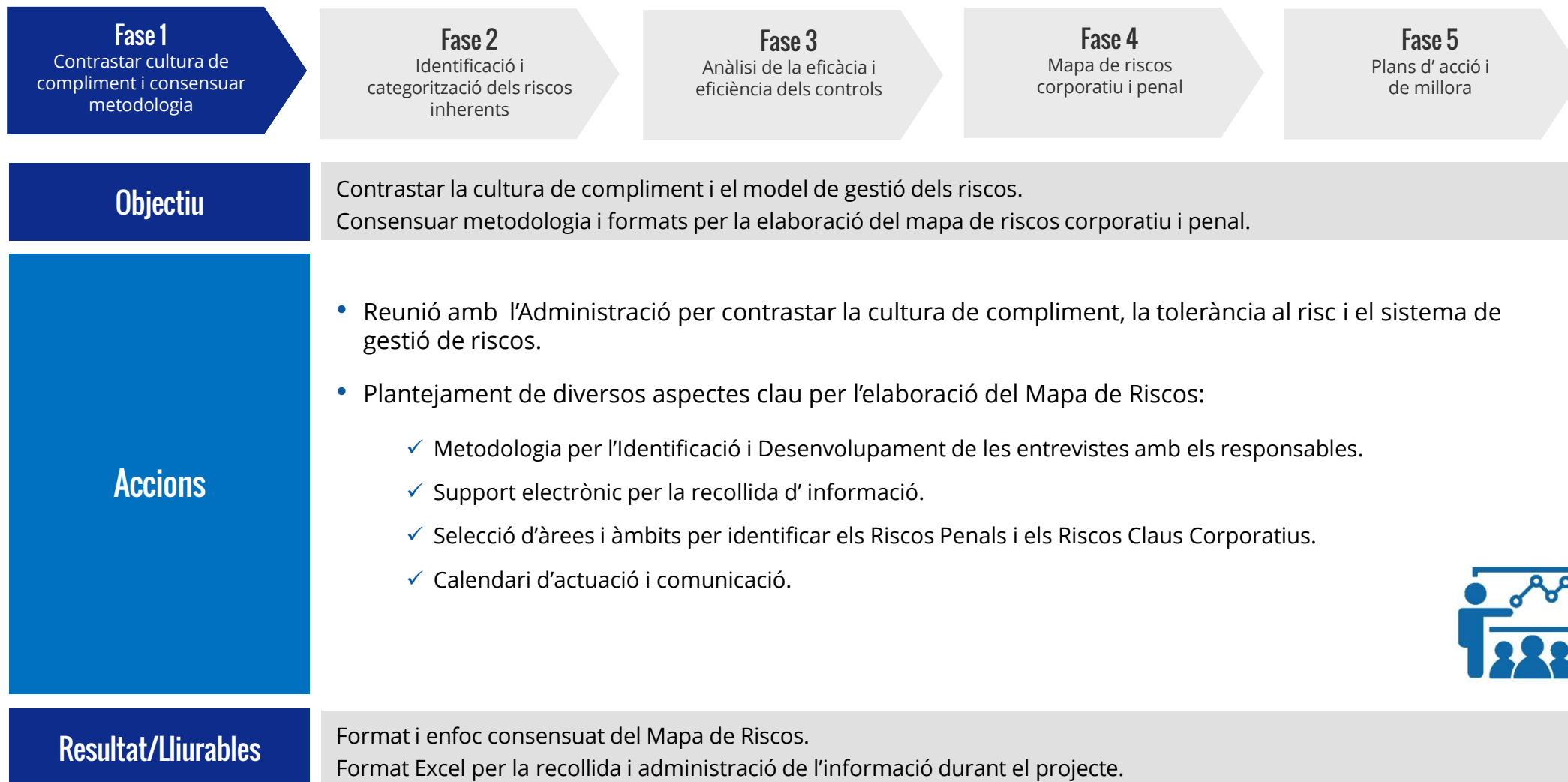


Treball intern
empresa

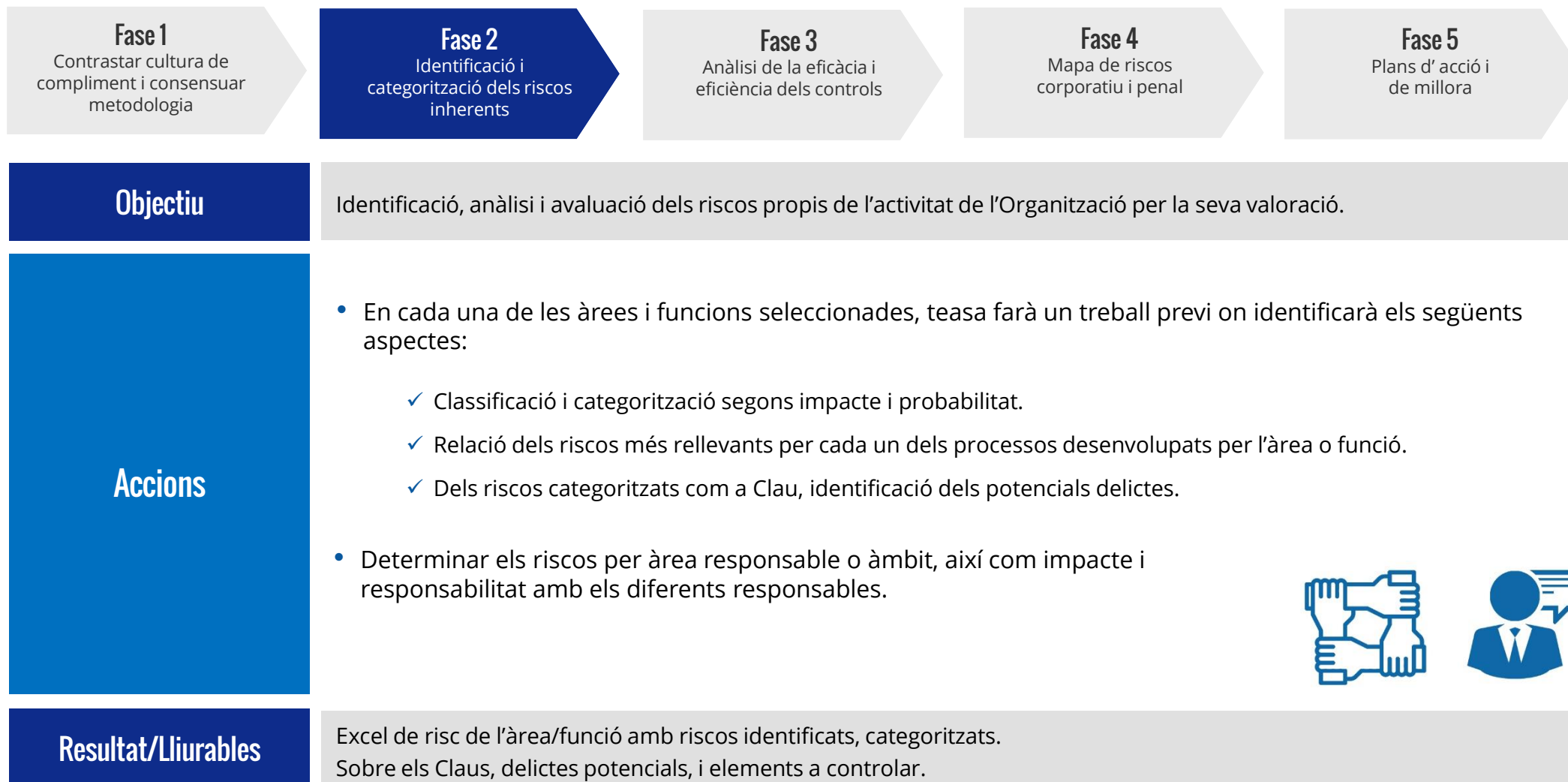


Treball consultor

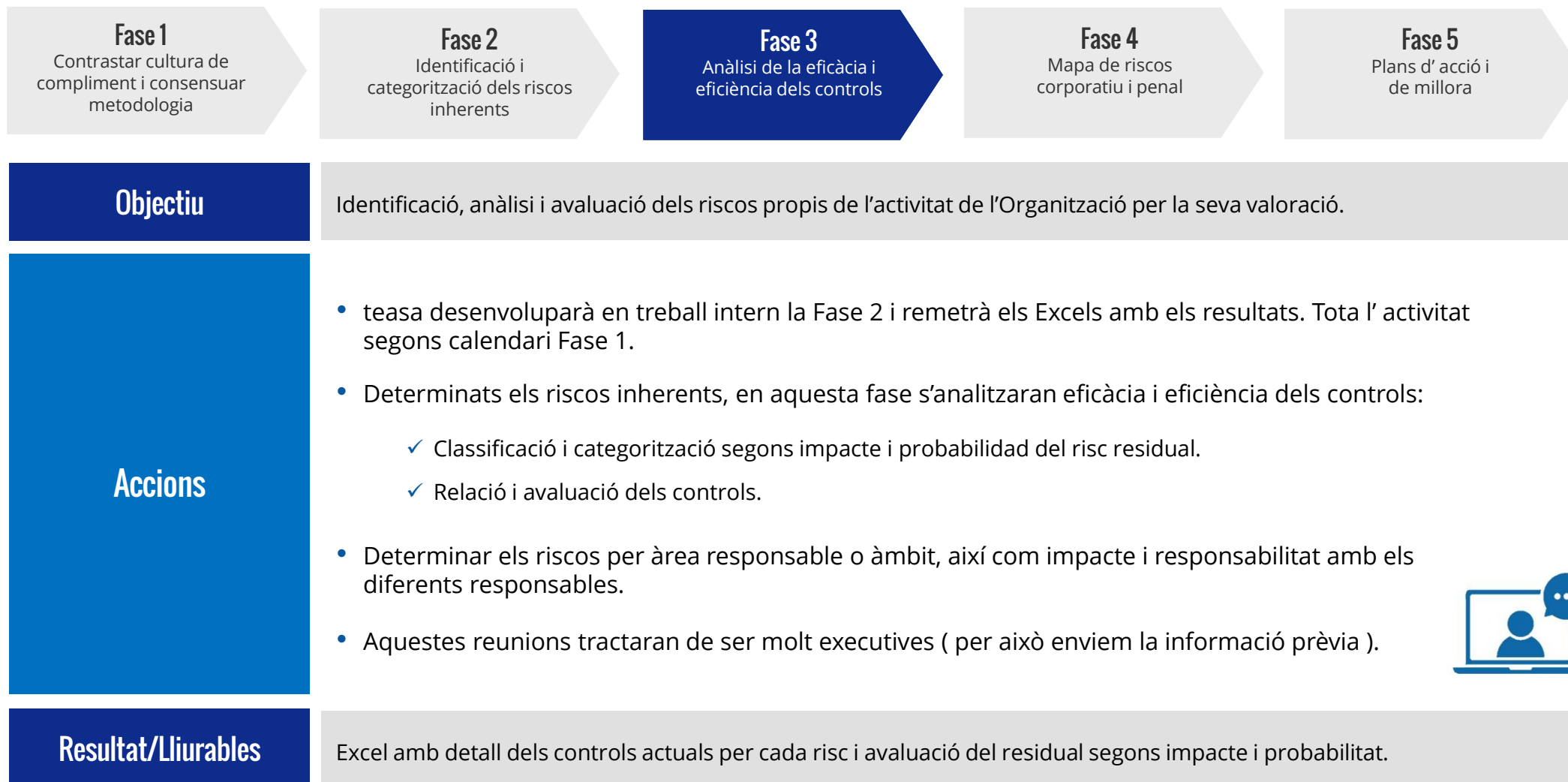
03 Desenvolupament del Projecte



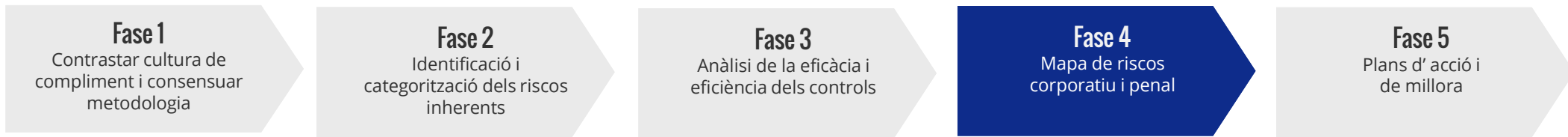
03 Desenvolupament del Projecte



03 Desenvolupament del Projecte



03 Desenvolupament del Projecte



Objectiu Elaborar Mapa de riscos penals i corporatiu.

Accions

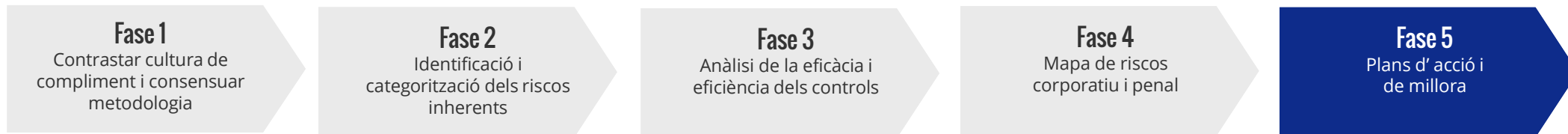
Resultat/Lliurables Excel amb Mapa de riscos corporatius i Mapa de color dels riscos penals.

Descripció del risc	Catòleg del risc	Tecnologia del risc	Impacte del risc	¿Es pot evitar el risc?	Impacte	Probabilitat	Puntatge risc (Impacte x Probabilitat)	Control Mitjà preventiu del risc	Impacte final con control	Probabilitat final con control	Puntatge risc final (Impacte x Probabilitat)	Nivell de severitat	Àrea/Departament de Responsabilitat	Riscs no pensats
Falta de política de seguretat IT (no documentada)	Operatiu	Tecnològic	NO		4. Alto	3. Ocasional	12	Enllaç elaborador Política. Se signa per el responsable del Departament. El Director de Àrea decideix les accions	4. Alto	2. Possible	8		Departament de Sistemes	
Falta de Política de uso de recursos tecnològics documentada (telèfon secure, dispositius, uso personal...)	Operatiu	Tecnològic	No		4. Alto	4. Alta	16		4. Alto	3. Ocasional	12		Departament de Sistemes	
Gestió de sistemes o "accidents" de informació/sistemes	Operatiu	Tecnològic	SI	Difícil Tecnològic	5. Crític	5. Muy alta	25	Fiscalització de sistemes, accés remot supervisat, tots actualitzats	5. Crític	3. Ocasional	15		Departament de Sistemes	
Incumpliment de la Ley de Protección Datos Personal	Operatiu	Tecnològic	SI	Difícil contra la intimitat y/o por revocación datos	4. Alto	2. Possible	8	CFO independiente para garantizar la seguridad de la información y evitar que vulneren sistemas de datos	3. Moderado	1. Poco probable	3		Departament de Sistemes	SI
Pérdida de datos o información asociada a sistemas. Seguridad de la información.	Operatiu	Tecnològic	SI	Difícil Tecnològic	5. Crític	5. Muy alta	25	Actualització de sistemes de seguretat	3. Moderado	1. Poco probable	3		Departament de Sistemes	SI

Impacte	Crític	5	5	10	15	20	25
	Alt	4	4	8	12	16	20
	Moderat	3	3	6	9	12	15
	Menor	2	2	4	6	8	10
	Insignificat	1	1	2	3	4	5
Probabilitat							
	Poc probable	Posible	Ocasional	Alta	Molt alta		
	1	2	3	4	5		



03 Desenvolupament del Projecte



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 adicional	▼	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