Checklist - Is uw bedrijf voldoende beveiligd tegen financiële criminaliteit?

WHISTLEBLOWER PARTNERS

Voer een controle uit door 20 vragen af te vinken of uw bedrijf voldoende beveiligd is tegen financiële criminaliteit.

Governance en risicobeoordeling

1. Is het bedrijf ooit slachtoffer geweest van financiële criminaliteit, onder meer door werknemers, of heeft het bedrijf zelf overtredingen van de wet begaan?

2. Beoordeelt het bedrijf voortdurend het risico om te worden blootgesteld aan financiële criminaliteit of dat de regels door medewerkers of op andere wijze worden overtreden?

3. Gebruikt het bedrijf extern juridisch of ander advies om ervoor te zorgen dat het bedrijf voldoet aan de wet (compliant is)?

4. Werkt het bedrijf zijn eventuele risicobeoordeling voortdurend bij?

Managementinformatie

5. Is er een beoordeling van het risico voor interne en externe fraude bij de controle door de externe accountant?

6. Heeft het bedrijf een compliancefunctie/verantwoordelijke?

7. Heeft het bedrijf een klokkenluidersregeling?

8. Is er iemand aangewezen om het risico van financiële criminaliteit aan te pakken?

9. Heeft het bedrijf inbraakalarmen, bewakingscamera's, toegangspassen en dergelijke om de fysieke veiligheid te garanderen?

Beleid en handleidingen

10. Zijn er beleid, richtlijnen, zakelijke procedures of procedures met betrekking tot het risico van financiële criminaliteit, waaronder

a) witwassen van geld en terrorismefinanciering,
b) fraudepreventie,

c) AVG en gegevensbeveiliging,
d) omkoping en corruptie,
e) schending van het mededingingsrecht,
f) financiële sancties, g) marktmisbruik,
h) belangenconflicten en
i) huiszoekingshandleiding

11. Worden het beleid en de procedures van het bedrijf regelmatig herzien?

12. Neemt het bedrijf initiatieven om ervoor te zorgen dat het personeel zijn beleid en procedures begrijpt?

13. Zorgt het bedrijf ervoor dat beleid, handleidingen en procedures enz. in het hele bedrijf worden verspreid en toegepast?

Werving, controle van medewerkers, training en bewustzijn en opleiding

14. Worden medewerkers bij hun aanstelling gecontroleerd op relevante risico's?

15. Worden de medewerkers geïnformeerd over, onderwezen in of getraind in bewustzijn over het risico van financiële criminaliteit, waaronder

a) witwassen van geld en terrorismefinanciering,
b) fraudepreventie,
c) AVG en gegevensbeveiliging,
d) omkoping en corruptie,
e) schending van het mededingingsrecht,
f) financiële sancties,
g) marktmisbruik en
h) belangenconflicten?

16. Heeft het personeel toegang tot training en opleiding over de relevante risico's van financiële criminaliteit?

Onboarding van klanten, leveranciers, agenten, resellers en andere derden

17. Zijn er systemen om zicht te houden op due diligence bij klanten, leveranciers, agenten, resellers en andere derden?

18. Is er bij het benaderen van klanten, leveranciers, agenten, resellers en andere derden due diligence uitgevoerd op basis van een concrete risicobeoordeling?

19. Wordt er doorlopend zicht gehouden op due diligence bij klanten, leveranciers, agenten, resellers en andere derden?

20. Wordt onderzocht wie de 'beneficial owners' zijn van klanten, leveranciers, agenten, resellers en andere derden?