



Tjekliste - Er din virksomhed tilstrækkeligt dækket ind over for økonomisk kriminalitet?



**WHISTLEBLOWER
PARTNERS**

Check ved afkrydsning af 20 spørgsmål, om din virksomhed er tilstrækkeligt sikret mod økonomisk kriminalitet.

Governance og risikovurdering

1. Har virksomheden været udsat for økonomisk kriminalitet, herunder fx af medarbejdere, eller har virksomheden selv foretaget overtrædelser af lovgivningen?
2. Vurderer virksomheden løbende risikoen for at blive udsat for økonomisk kriminalitet eller for selv gennem medarbejdere eller på anden måde at overtræde regler?
3. Bruger virksomheden ekstern juridisk eller anden rådgivning for at sikre, at virksomheden overholder lovgivningen (er compliant)?
4. Opdaterer virksomheden løbende sin eventuelle risikovurdering?

Ledelsesinformation

5. Indgår der en vurdering af risikoen for intern og ekstern svindel i ekstern revisors revision?
6. Har virksomheden en compliancefunktion/ansvarlig?
7. Har virksomheden en whistleblowerordning?
8. Er der udpeget en ansvarlig for håndteringen af risikoen for økonomisk kriminalitet?
9. Har virksomheden tyverialarmer, overvågningskamera, adgangskort og lignende for at sikre den fysiske sikkerhed?

Politikker og manualer

10. Findes der politikker, guidelines, forretningsgange eller procedurer vedrørende risikoen for økonomisk kriminalitet, herunder
 - a) hvidvaskning af penge og terrorfinansiering,
 - b) forebyggelse af svig,
 - c) GDPR og datasikkerhed,

- d) bestikkelse og korrupsion,
- e) overtrædelse af konkurrencelovgivningen,
- f) økonomiske sanktioner,
- g) markedsmisbrug,
- h) interessekonflikter og
- i) Dawn Raid manual

11. Gennemgås virksomhedens politikker og procedurer med jævne mellemrum?

12. Tager virksomheden initiativer til at sikre, at personalet forstår dets politikker og procedurer?

13. Sikrer virksomheden, at politikker, manualer og procedurer mv. formidles og anvendes i hele virksomheden?

Rekruttering, kontrol af medarbejdere, træning og opmærksomhed og uddannelse

14. Bliver personalet ved ansættelse checket for relevante risici?

15. Bliver medarbejderne informeret om, undervist i eller trænet i opmærksomhed overfor risici for økonomisk kriminalitet, herunder

- a) hvidvaskning af penge og terrorfinansiering,
- b) forebyggelse af svig,
- c) GDPR og datasikkerhed,
- d) bestikkelse og korrupsion,
- e) overtrædelse af konkurrencelovgivningen,
- f) økonomiske sanktioner,
- g) markedsmisbrug og
- h) interessekonflikter?

16. Har personalet adgang til træning og uddannelse i de relevante risici for økonomisk kriminalitet?

Onboarding af kunder, leverandører, agenter, forhandlere og andre 3-mænd

17. Findes der systemer til gennemførelse af due diligence vedrørende kunder, leverandører, agenter, forhandlere og andre tredjemænd?

18. Bliver der ved tilgang af kunder, leverandører, agenter, forhandlere og andre 3-mænd gennemført due diligence baseret på en konkret risikovurdering?

19. Bliver der løbende i et forhold til kunder, leverandører, agenter, forhandlere og andre 3-mænd gennemført due diligence?

20. Bliver det undersøgt, hvem der er "beneficial owners" af kunder, leverandører, agenter, forhandlere og andre 3-mænd?