Checklist - Is your company adequately protected against financial crime?

WHISTLEBLOWER PARTNERS

Determine whether your business is adequately protected against financial crime by ticking off answers to 20 questions.

Governance and risk assessment

1. Has the company been the victim of financial crime, including by employees, or has the company itself committed violations of the law?

2. Does the company continuously assess the risk of being subjected to financial crime or of violating rules itself through employees or otherwise?

3. Does the company use external legal or other advice to ensure that the company is compliant?

4. Does the company update its risk assessment regularly, if such an assessment exists?

Management information

5. Does the external auditor's audit include an assessment of the risk of internal and external fraud?

6. Does the company have a compliance function/officer?

7. Does the company have a whistle-blower scheme?

8. Is there a designated person responsible for managing the risk of financial crime?

9. Does the company have burglar alarms, security cameras, access cards and the like to ensure physical security?

Policies and manuals

10. Are there policies, guidelines, business processes or procedures in place relating to the risk of financial crime, including

a) money laundering and terrorist financing,
b) fraud prevention,

c) GDPR and data security,
d) bribery and corruption,
e) breach of competition law,
f) financial sanctions,
g) market abuse,
h) conflicts of interest and
i) Dawn Raid manual

11. Are company policies and procedures reviewed regularly?

12. Does the company take measures to ensure that staff understand the company's policies and procedures?

13. Does the company ensure that policies, manuals and procedures, etc. are communicated and applied throughout the company?

Recruitment, employee checks, training and awareness

14. Are staff checked for relevant risks on recruitment?

15. Are employees informed, educated or trained in awareness of financial crime risks, including

a) money laundering and terrorist financing,
b) fraud prevention,
c) GDPR and data security,
d) bribery and corruption,
e) competition law violations,
f) financial sanctions,
g) market abuse and
h) conflicts of interest?

16. Do staff have access to training and education on relevant financial crime risks?

Onboarding of customers, suppliers, agents, resellers and other third parties

17. Are there systems in place to carry out due diligence on customers, suppliers, agents, resellers and other third parties?

18. When customers, suppliers, agents, resellers and other third parties are brought in, is due diligence carried out based on a concrete risk assessment?

19. In relationships with customers, suppliers, agents, resellers and other third parties, is due diligence conducted on an ongoing basis?

20. Are the identities of "beneficial owners" of customers, suppliers, agents, resellers and other third parties looked into?