The Institute of Internal Auditors Australia

The 20 Critical Questions Series

What Directors should ask about Compliance

Updated 2022

Compliance Foundations

1. Does the organisation have a comprehensive compliance framework? Does it include a specific compliance policy including charter or terms of reference for the compliance activity and is the policy approved by the board of directors? Are there approved critical success factors or performance measures (KPIs) for the compliance activity?
2. Does positioning within the organisation give the compliance activity reporting avenues independent of line management?
3. Is there a specified person or activity in the organisation responsible for compliance? Are the people working on compliance skilled and suitably qualified specialists rather than generalists?
4. Is the organisation conforming with the standard ISO 37301:2021 'Compliance management systems – requirements with guidance for user?
5. Is there an awareness program to assure people inside and outside the organisation know their legal obligations and policy requirements? Is this reflected in (a) internal – job descriptions, performance measures, etc (b) external – tenders, contracts, etc?
6. Is there a risk-based compliance work plan approved by the audit committee that aims to assure legal obligations and policy requirements are met? Does the compliance work plan extend to subsidiaries, and controlled and associated entities?
7. Are compliance non-conformances recorded, allocated to appropriate management for corrective action, and regularly followed-up? Are breaches reported to the audit committee and regulators where necessary on a transparent and timely basis? Is corrective action progress regularly reported to the audit committee?
8. Are compliance obligation results regularly reported to executive management for (a) legal compliance (b) policy compliance? Are compliance obligation results regularly reported through independent assurance activities to the audit committee and board of directors? Does this include a compliance annual report that contains performance measure results and an attestation statement from the compliance activity?

Legal Compliance

9. Does the organisation have a compliance register listing all laws and parts of those laws it needs to comply with? Is it risk-rated, contain existing controls, and also planned further controls where risk needs to be reduced in line with the organisation's approved risk appetite?
10. Does the organisation have a process to make sure new and changed legal requirements are brought to the organisation's attention and promptly reflected in the compliance register?
11. Are there review activities in place to periodically confirm the organisation complies with applicable laws and maintains its related policies and procedures up-to-date?
12. Is executive management required to provide a sign-off to the audit committee and board of directors each year that the organisation is complying with all applicable laws?
13. Does the organisation record in a register and actively follow-up all legal proceedings involving the organisation?
14. Is the organisation engaged in joint ventures that introduce compliance risk? How does the organisation ensure that joint ventures understand and apply the corporate values? How does the

What Directors should ask about their Audit Committee

organisation know it is in compliance with joint venture agreements, especially where operations of the joint ventures extend across international borders?

15. Is there exposure to international laws? If so, how is compliance assured and reported?
16. Is there compliance with public disclosure and whistleblower law requirements? Are there review activities in place to periodically examine compliance with other external obligations such as (a) anti-corruption law (b) anti-money laundering and counter-terrorism financing law (c) foreign bribery law (d) privacy law (e) modern anti-slavery law?
17. Is management confident that suitable training and awareness programs are in place so staff and suppliers are familiar with their compliance obligations, including changes as they arise, and these obligations are reinforced periodically?

Policy Compliance

18. Is there a formal organisation process for policies including a 'policy on policies' to assure policies are consistently developed, risk rated, implemented, applied, reviewed and maintained up-to-date?
19. Is there a risk-based process to ensure policy compliance is periodically assured and audited?
20. Is there a risk-based process to ensure policies are periodically reviewed and maintained up-to-date? Are results reported to executive management and the audit committee?

The Big Question

How does management, the audit committee and board of directors clearly know the organisation is complying with all legal obligations and policy requirements across its operations and its broader remit?