



A Checklist: Identifying Red Flags in Your Regulatory Intelligence Strategy

62% of general counsels say their organization's risk exposure is changing more quickly than it was 12 months ago, according to a Gartner survey.

For corporations today, failure to keep up with an increasing regulatory burden carries implications beyond fines. Noncompliance can incur political risk, which can then negatively impact operations, cash flow, profitability, and more.

Business agility may also be affected. Expanding into a new market requires knowledge of jurisdiction-specific rules in financial reporting, data privacy, the environment, and beyond.

This knowledge is referred to as "regulatory intelligence," which guides the strategic decisions today's corporate boards, executives, and legal teams make. When companies have gaps in their regulatory intelligence strategy, they risk many things: missing red flags, incurring costly penalties for noncompliance, impeding board oversight, hindering decision-making across audit, tax, and legal teams, and so on.

The first step towards better regulatory intelligence is identifying gaps. Here are 10 red flags that may indicate bigger problems:

- 1. Regulatory reporting for the corporation's entities is neither standardized nor integrated.** This can leave the organization vulnerable to information gaps and inhibits organizations from maintaining a "single source of truth."
- 2. Board communication for regulatory oversight lives in spreadsheets and personal documents.** These methods are disconnected and pose significant security risk.
- 3. Regulatory and compliance information regularly fails to flow in a timely manner.** Time is money when it comes to regulatory compliance. Time also increases risk. A lack of prompt intelligence impairs decision-making across the organization.
- 4. The organization possesses insufficient tracking for important areas like professional licensing, FCPA compliance, and sexual harassment training.** Management lacks a full picture of policy compliance and risk exposure—and can't escalate problems to the board in a timely fashion.
- 5. Information on regulatory compliance is not transparent.** Top executives and directors lack full access to the overall regulatory landscape.
- 6. Compliance information is cumbersome to access.** The inability to generate quick reports becomes problematic in time-sensitive situations like audits and regulator requests.
- 7. Regulatory information is neither stored nor communicated securely.** This leaves organizations vulnerable to both cyberattacks and the risk of missing a red flag.
- 8. The board and top executives are regularly surprised by regulatory trends and developments.** Reporting features must support the GC, audit, and legal teams in providing visibility across company leadership.
- 9. Internal regulatory issues aren't being discussed until it's too late.** Too often, red flags are missed—or take too long to identify. Consequences can range from fines to negative attention to activist scrutiny.
- 10. The board is not mapping regulatory compliance to corporate strategy.** For mergers and acquisitions, policy oversight, risk management, and more, directors don't have the insights they need to excel in their oversight role.

Navigating the many facets of today's risk landscape requires specialized technology. A comprehensive software solution can help centralize, synthesize, and protect corporate processes related to regulatory compliance, risk monitoring, board management and reporting, and competitive intelligence.

Learn more: [Security, Risk, and Compliance: What to Look for In a Technology Solution](#)

For more information or to request a demo, contact us today:
Email: info@diligent.com | Call: +1 877 434 5443 | Visit: diligent.com