Published on *The National Law Review* https://natlawreview.com

Five Keys to a Successful Compliance Risk Assessment

Article By:

Sarah E. Aberg

J. Scott Maberry

Corporate compliance programs are expected to be tailored to an organization's unique risks. Most regulators (and most modern organizational compliance programs) prescribe risk-based compliance. But one thing is to prescribe; another is to execute properly.

Based on our experience with dozens of major organizations, this article provides five keys to a successful compliance risk assessment:

1. Detect and measure the broadest range of risks

No two organizations have the same risk profile. And the vastness of the potential problems can sometimes be overwhelming. But it is important to cast a broad net. Don't let confirmation bias or other cognitive illusions limit you. Think about the wide range of factors affecting your risk, including business activities, market forces, regulatory landscape, geographic locations, reliance on third parties, potential clients and business partners, and the categories of data maintained and transmitted by the company.

Once detected, risks may be rated and ranked in terms of severity. For example, a company maintaining confidential customer data (e.g., biographic, financial, or medical information), faces cybersecurity risks. But the volume, content, and means of collection and maintenance of the data will affect whether the risk is high, medium, or low. For tips on measuring and ranking risk, see our paper on the principle of "Measure What You Manage."

Some of the severest risks are detected only after the fact. Consider conducting a "Legal Pre-Mortem " to put yourself in a position of "prospective hindsight" to identify emerging risk.

2. Identify the consequences

The consequences your organization could face are defined by the regulatory and enforcement landscape. Many risk activities are subject to multiple regulatory regimes, and enforced by multiple agencies. Even in the absence of regulation, private litigation is a potential consequence of risky behavior. Some regulatory regimes create private rights of action, bringing together both public and private-driven consequences. In the realm of customer data, for example, if the organization fails to take reasonable steps to protect data, it may face civil enforcement actions by the relevant regulators (e.g., a public company is subject to the Securities and Exchange Commission's cybersecurity requirements; New York State-licensed financial institutions are subject to the State's Department of Financial Services cybersecurity requirements). However, a breach could also be the basis for a criminal insider trading investigation by the U.S. Department of Justice or state law enforcement. Finally, the company could be subject to individual or class action claims if personal consumer data is compromised or stolen.

Anticipating and accounting for all potential consequences requires comprehensive knowledge of the regulatory landscape.

3. Assign ownership

Assigning ownership of risks is another key to successful risk assessment. Ownership of risk comes in two flavors: those whose activities create the risk and those who manage those risks. Your risk management program should recognize both roles. Returning to our cybersecurity example, every employee with a company email address is a potential phishing scam target. The employees are responsible for exercising reasonable diligence and care when opening and responding to emails. But management is responsible for ensuring the employees have adequate training and resources to recognize and report email scams. Management must also maintain competent IT staff and technology to proactively flag and combat such scams. The board has responsibilities also, including ensuring that the proper controls are in place and properly resourced and tested.

4. Match controls to the risks

The menu of risk mitigation steps is infinite. The gamut includes policy statements, training, automated alert systems, compliance staffing, audits, direct board oversight, and everything in between. The budget for compliance is finite, however. This means you may need to get creative in matching controls to the risks. Typically, a control can be defended if it is "reasonably designed" to address the risk. But it is imperative to accurately match the mitigating value of the control commensurate to the severity of the risk. For example, a policy statement asserting that the company will take all necessary steps to protect sensitive data will have little mitigating effect on high-risk activities that involve collecting and maintaining substantial volumes of such data. If you've identified a risk without a reasonable mitigating control, you'll need to devise a plan to address it. While it may well be an issue the organization can handle internally, some newly-identified risks may require more robust review, including a lookback to determine the extent of any harm as a result of the gap. Sometimes this requires engaging expert counsel to advise on reporting and regulatory obligations.

5. Fill the gaps

All the keys outlined here can help organizations identify and address gaps in existing risk management infrastructures. An effective risk assessment is dynamic and allows organizations to identify risks that may not be covered by its existing controls. This could happen both when new risks are introduced (such as a new product line or business activity) or the nature of the risk changes (because the activity has been outsourced to a vendor, or there has been a material change in business or operational processes). The risk assessment process should account for changes in the regulatory and enforcement landscape, and be informed by historical performance. Organizations should evaluate effectiveness based not only on internal performance, but also external incidents.

Though your company may not have had a cybersecurity incident, if another company using similar controls did succumb to an attack, your risk assessment should include a reevaluation of those controls and incorporate any “lessons learned” from that incident, notwithstanding it happened to someone else.

One final takeaway: try to tie your risk mitigation steps to your company’s organizational culture and values. This has been one of the most striking observations we have seen from advising organizations on existential compliance threats. There is a strong body of research demonstrating that aligning risk mitigation obligations with core beliefs improves judgment, enhances decision making, and creates the most successful outcomes.

The aim in all of this is to reach a point at which your organization has taken reasonable steps to identify the risks and those risks are reasonably controlled. This does not mean a guaranteed control for every conceivable risk. Rather, it means reasonable controls that are tailored to the severity of the risks. If, for example, a company has conducted bi-monthly training and incident response scenarios for employees, managers, and directors, with no incident history, it may be reasonable under the circumstances to reduce such training to an annual or semi-annual schedule. There may even be certain low-risk activities that require no additional controls beyond a policy statement. Whatever the ultimate result and decision, above all, it must be well-reasoned and documented. Memorializing the risk assessment properly can position your organization well to respond to regulators and law enforcement, even in the event of an incident.

National Law Review, Volume XI, Number 96

Source URL:https://natlawreview.com/article/five-keys-to-successful-compliance-risk-assessment