Deloitte.

Enterprise compliance
The Risk Intelligent approach

The compliance agenda starts here

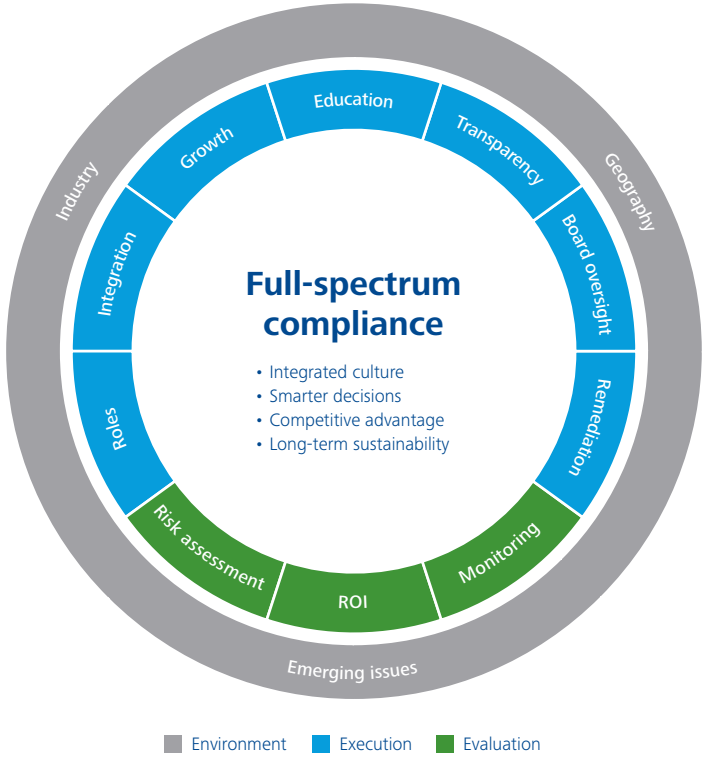
As globalization continues to take hold and government regulation broadens around the world, spilling across country borders, the issue of compliance risk remains a top-shelf business issue. It's not just an item on the agenda. Compliance is its own agenda these days.

And with good reason. Given the pace and scale of change they're facing, senior executives and boards are more concerned than ever that the old, reactive ways of managing compliance may cause them to fall behind the competition – or leave them exposed to greater regulatory or reputational risk than ever. Meanwhile, the world keeps turning. Forward-thinking leaders are looking for ways to make their organizations more Risk Intelligent.

Enterprise compliance spanning multiple businesses, organizational units, and geographies is increasingly seen as the goal for organizations looking to act in an ethical manner and keep compliance risk in check. In this book, we offer what we believe to be the core elements of a compliance agenda that supports the whole enterprise.

Who is this for?
This book is for senior business leaders and board members who are pursuing a leading compliance capability, regardless of whether their organizations are highly regulated, unregulated, public, or private. It was informed by years of discussions and work at some of the world's leading companies.

Throughout this book, we have included unattributed quotes taken directly from our conversations with many of these leaders. For those of you who recognize your words, thank you for your time and insight.


Education
Transparency
Board oversight
Remediation
Monitoring
ROI
Risk assessment
Roles
Integration
Growth
Industry
Geography
Emerging issues
Full-spectrum compliance
• Integrated culture
• Smarter decisions
• Competitive advantage
• Long-term sustainability
Environment
Execution
Evaluation

Covering the full spectrum

Enterprise compliance is a coordinated approach to compliance spanning multiple businesses, organizational units, and geographies, enabled by people, processes, and technology. The goal? An integrated model of compliance across the organization that helps ensure ethics are being followed at every level.

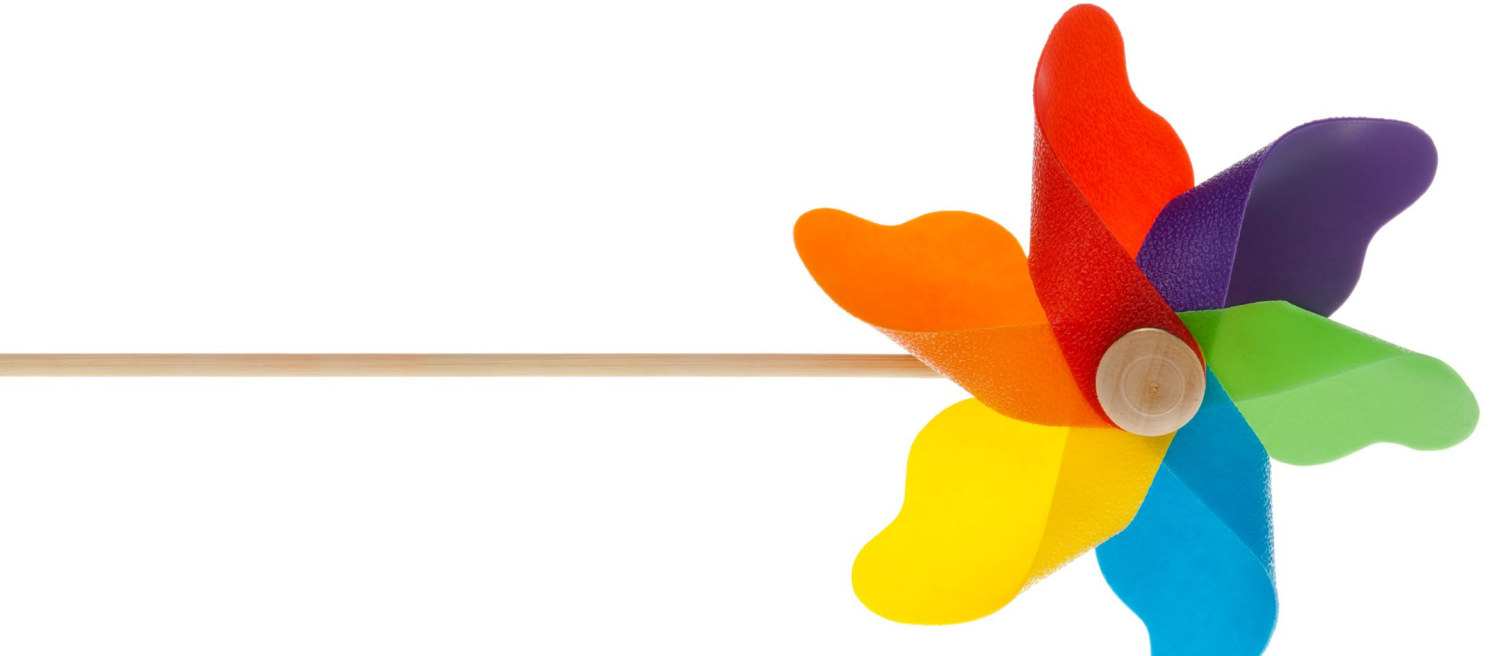
That's the approach top executives and board members want and should take.

Getting it done

Effective compliance isn't just reflected in an organization's ability to check all the right boxes. It's reflected in employees' willingness to do the right thing. Creating this culture of compliance is the result of all of the core components shown on the previous page.

In this book, we explain the role each of them plays in creating a compliance culture, by category: environment, execution, and evaluation. We've also included the tough questions board members tell us they're asking about these issues. If you're a senior executive, use these questions as a guide to your next in-depth discussion on compliance risk.

Environment



Industry

The biggest driver of an organization's compliance risk and requirements is typically its industry footprint. Companies in the same industry, of roughly the same size, may be facing very similar compliance challenges at any given moment. Just as important, they may be sharing an equally similar playbook. But when you're looking to lead the pack, sharing the same strategies as your competitors won't do. How can business leaders and board members establish a compliance strategy rooted in industry, without taking the exact same approach as close competitors?

It helps to start with a measuring stick: *What are our peers doing? How do we match up across key benchmarks?* The next step should be to zero in on what the organization is doing differently (good or bad) around compliance risk today and what it should be doing differently tomorrow. That exercise should include an accounting of the organization's complete industry footprint and corresponding compliance risk. Given the size and complexity of many businesses today, the executive team may not have a clear understanding of how their industry footprint impacts compliance risk. Regardless of the industry, there are ways to drive more value from compliance beyond simply following the rules.

For example, executive leadership may advocate a compliance strategy that anticipates future industry trends across businesses, products, services, or geographies. Such an approach could help the organization establish a competitive advantage through well-planned programs that take on new rules, sidestepping an inefficient, last-minute scramble to comply. While others are trying to keep up, they could be focused on the road ahead.

> "We handle compliance like everyone else in our industry. So how do we gain an edge?"

Must-ask questions

- ☐ Who can give me a detailed snapshot of all the compliance issues we face, given our specific industry footprint? What should our priorities be? How do we know?
- ☐ Who's the best in our industry? How are they better – and why aren't we that good?
- ☐ How are our requirements unique among our competitors? How do we know that?
- ☐ Which organizational structures have we considered for our compliance management approach? Why did we choose the one we have in place today?
- ☐ What regulatory changes are likely to affect our business in the future, and what are we doing today to address them?
- ☐ How are new players in our industry innovating to address their compliance risks?

Geography

Even if your company had just one location, avoiding the influence of geography on your compliance strategy would still be difficult. Compliance issues extend as far as your products or services are offered and throughout the entire supply chain. Where are your materials sourced? Where are your key partners or suppliers located? Where are your customers? You get the idea.

Adding to the complexity, different cultures have different ideas about what constitutes adherence and corruption. An enterprise compliance approach can be difficult to enforce when there are such stark differences around the world. Also consider that this complexity does not stop at the country level. In the U.S., for example, different states enforce different regulatory guidelines, and cities and counties will often add more layers to suit their own requirements.

In the end, the issue of geography is virtually inextricable from growth. Any conversation about the impact of geography on compliance efforts has to simultaneously account for plans for growth. Because your geography is not just a reflection of the organization's current footprint – it's about the future state as well. And there's no way to plan for that without understanding the growth strategy.

> "I believe that our corporate standards should be the same, no matter which country we're operating in."

Must-ask questions

- ☐ What does our entire supply chain or sourcing footprint look like?
- ☐ What are the most complex domestic regulatory issues we face, and how do they differ in other geographies?
- ☐ How does our industry footprint vary by geography?
- ☐ Which compliance issues are third parties around the world exposing us to?
- ☐ How are we monitoring pending changes and legislation that might affect us at the global level? What about at the state, province, or even municipal level?
- ☐ How is compliance integrated into our geographical growth strategy and tactics?
- ☐ In which countries are we most vulnerable to compliance risks? How are we addressing these vulnerabilities?
- ☐ How do we export our compliance culture and code of ethics to other geographies?

Emerging issues

As with any risk, when it comes to compliance, it's often the new issues no one anticipated that present the biggest challenges. But just because no one saw it coming doesn't mean someone *couldn't* have. Too often, compliance efforts are focused on the steady state of the business. How can business leaders and board members make sure they're prepared for emerging issues as well?

While many parts of the business are consumed with anticipating emerging issues, such an approach is not typically the domain of the compliance function. Too often, compliance is all about what's happening today, and what happened in the recent past. Who has the time and resources to worry about what could be around the corner?

The good news is that it's not nearly as difficult as it used to be to stay a step ahead of emerging compliance trends, given the growing number of tools and technologies available today. They can point to critical, current risks and help identify future shifts before they impact the business.

Of course, technology alone is never enough. With the right people and processes in place, it can be easier to consistently determine what to look for, where to look for it, and how to address it.

> "Our business is changing all the time. How is our compliance strategy changing with it?"

Must-ask questions

- ☐ What's changing – and what's our game plan for changing with it?
- ☐ How do we research and prepare for what's happening in the future?
- ☐ How is compliance incorporated into our five-year business plan?
- ☐ How are compliance trends incorporated into our growth decisions?
- ☐ How are we identifying, monitoring, and adjusting for emerging compliance risks and requirements?

Execution

Roles

"Everyone's responsible for compliance." Heard that before? If management believes everyone is responsible, there's a chance that in reality, nobody's at the wheel. Yes, compliance needs to be on everyone's radar. But some people have more responsibility than others.

In the real world, ownership of compliance tends to disappear only a few layers deep into the organizational chart, becoming less visible the further you move away from core compliance functions and roles such as the Chief Compliance Officer. As a result, employees in business units and functional operating units may be performing compliance-related activities every day without knowing the potential consequences of not executing them properly.

Just as important, when processes are updated, or workarounds are put in place, critical compliance tasks may be inadvertently eliminated without anyone understanding the impact on compliance risk. Pushing responsibilities closer to the front lines of the business can make the overall process of compliance more efficient and less painful, but it can also bring new headaches without adequate planning.

One of the leading ways to avoid the unintended consequences that can come from changing responsibilities is to start with a complete picture of how compliance works in an organization. It can be difficult, but the confusion and risks of operating without such an understanding can be even more painful. From there, make sure people know what they are expected to do and why, and provide them with the incentives they need to stay on track.

> "When I asked our board where responsibility for compliance risk resided, they looked around and said, 'It doesn't reside anywhere. That's an issue for management, not the board.'"

Must-ask questions

- ☐ Who is ultimately responsible for compliance? How are they held responsible?
- ☐ How are different functions such as compliance, internal audit, HR, risk management, tax and legal integrated?
- ☐ How does our compliance program work? Explain it in 50 words or less.
- ☐ What's the role, accountability, and scope of authority of the compliance officer? Is that person sufficiently independent of management? To whom does he or she report?
- ☐ How are authority and accountability enforced? How are these issues built into performance appraisals?
- ☐ How is ownership of compliance defined throughout the organization?
- ☐ How are we managing third-party responsibilities for compliance risks?

Integration

On some level, every organization struggles with duplication of effort, and the inefficiencies and high costs that come with it. In compliance, the benefits of a consistent framework and tight integration with the business can be significant. It's not just about a smoother, less expensive approach to compliance. It's about delivering real value to the business, which is exactly where many compliance initiatives fall short. As with other parts of the business, establishing enterprise-level management and communications standards and frameworks can go a long way toward driving efficiency, control, and knowledge.

Compliance efforts driven separately from individual business units can appear to be efficient and fully integrated to those who are running them. But for others with a more objective vantage point, duplications and inconsistencies are more apparent. The costs of such a lack of integration – financial and otherwise – can be significant. The executive team and board are uniquely positioned to identify and help remedy these kinds of problems, using a combination of processes and technology to help make sure nothing is falling through the cracks. Incentives are another important tool leaders can use to eliminate siloes and drive a more integrated approach.

Integration becomes even more important when a large number of new employees or business activities are introduced into the organization through an expansion or acquisition. Smart leaders include compliance in their overall integration plans – and they take advantage of the opportunity to reconsider their own processes, mining leading practices from the acquired firm.

"Compliance has more moving parts than I can count. How do we make sure they're integrated with one another?"

Must-ask questions

- ☐ What exactly are we doing to identify and eliminate inefficiency and duplication in our compliance programs?
- ☐ What is the cost if we don't do anything further when it comes to compliance integration?
- ☐ We know we've made integration mistakes before – how are we learning and improving from those mistakes?
- ☐ What is the number of compliance programs we have in place today, and why is the number more than one?
- ☐ How can we use our upcoming acquisition to streamline and integrate our compliance program?
- ☐ What degree of integration do we actually want or need to achieve?
- ☐ How are we using technology platforms to drive greater integration in our approach to compliance?
- ☐ How are international locations and recent acquisitions incorporated into the compliance process?

Growth

Mergers. Acquisitions. New market and product offerings. Geographic expansion. Every play in the growth playbook has the capacity to reshape your compliance universe and introduce new types of compliance-related risks. In fact, some of them have the potential to derail or delay the entire strategy. Imagine committing resources to the launch of a new product or service before realizing or planning for the full extent of rigorous regulations it will require.

Compliance fears should never override the pursuit of growth. But they must inform that pursuit at every turn: when developing the business case, driving risk analysis, conducting due diligence, influencing return on investment (ROI) expectations, and contributing to key decisions and planning strategies along the way.

For example, consider the long list of considerations that shape and inform virtually any growth strategy. Structure – partnerships, agents, sales offices, joint ventures, and so on. Geopolitical challenges. Infrastructure. Corruption threats. Each of these issues introduces its own set of compliance challenges and opportunities. But in the pursuit of new growth, companies may underestimate the compliance angle in these areas. Today, that can be a recipe for disaster.

"I'm worried that too much is left to chance."

Must-ask questions

- ☐ What is the optimal organizational structure to support our geographical expansion?
- ☐ As we pursue our growth strategy, how are we identifying and addressing the new compliance requirements that will come with it?
- ☐ When identifying leaders for our new products and services, how do we account for their compliance track record?
- ☐ When we make an acquisition, how do we communicate our expectations for performance with integrity?
- ☐ How are we evaluating the compliance footprint of our mergers and acquisitions (M&A) opportunities?

Education

Just because the executive team and board are focused on compliance doesn't automatically mean that the rest of the organization even knows it's an issue on the radar. When it comes to compliance, many don't know where to focus, what their priorities should be, or how their performance will be measured. It can be a constant struggle to get those on the front lines to understand and care about compliance risks. That's where education comes in.

How is leadership communicating expectations and values when it comes to compliance? It often takes a wide range of activities for communications to break through to the front lines. Leadership town halls, for example, in which compliance plays a starring role. Visibility in offices and on the intranet. Clearly defined performance standards, evaluation criteria – and the rewards or consequences that come as a result of an evaluation. And more.

Training also has a role to play. While compliance issues are included in many training plans, are they really effective? For some companies, entire training curricula are dedicated to compliance – it's no afterthought. Those organizations are much more likely to create a culture of compliance from the top down and the ground up.

"We're not trying to teach the test. We're trying to change the culture."

Must-ask questions

- ☐ What are we doing to make sure our employees understand their responsibilities when it comes to compliance?
- ☐ How are we working to institutionalize a deep, broad culture of compliance? How are we measuring progress toward this goal?
- ☐ How is the 'tone at the top' carried throughout the organization?
- ☐ Where in each job description is the individual's responsibility on compliance clearly spelled out?
- ☐ How are we making sure that people know what is expected of them individually, from their first day forward?
- ☐ What role does training play in creating a culture of compliance in our organization?

Transparency

As compliance grows in importance, internal stakeholders such as the board and employees aren't the only ones who need to know how it's being addressed. There are a host of external groups who also have a keen interest in better understanding what's going on behind the scenes. Regulators, shareholders, business partners, collaborators, ratings agencies, the media, nongovernmental organizations, even interest groups – without properly meeting their needs, they could transform from being observers and advocates to adversaries.

It doesn't have to be that way.

Increased transparency about compliance – even about compliance failures – can improve the trust that stakeholders have in the organization and its leadership. And it's not just about avoiding fines and penalties. It's about broadcasting the fundamental ethics of the organization and the commitment to uphold those ethics. If outsiders understand and share your belief in those ethics, they're more likely to feel a strong connection to your organization. And in the event that a compliance mistake occurs, they'll be more likely to stand by you.

While there's no way to fully control the perceptions that stakeholders have about your organization, candid and consistent disclosures can make a big difference.

Must-ask questions

- ☐ What information do stakeholders want, how much detail do they need, and can we give it to them?
- ☐ Which compliance issues are most important to our customers? Shareholders? Business partners? Regulators? The media?
- ☐ What are we comfortable making public – and where do we draw the line?
- ☐ Which communications avenues and channels will we use for sharing information?
- ☐ What are we already reporting to the world through informal channels? Do we need to rein it in, and if so, how?
- ☐ Where have we fallen short in compliance reporting, and how are we addressing the problem?
- ☐ Who else outside our company is providing this information to our stakeholders? How are they getting it, and how are they sharing it?

Board oversight

There's no question the board has a big role to play in compliance. Plus, not only do its members have responsibility for compliance oversight, their individual reputations are on the line, along with those of the companies they oversee. How can they carve out an active role without going too far?

It can be too easy for board members to fall into the trap of managing compliance risk themselves, or to stand too far back and allow a risk management vacuum to develop. The rules of engagement must be clear, drawing a bright line between the roles of board members in providing oversight and those of the executives who are responsible for driving compliance day in and day out. To properly monitor the compliance programs of the company, the board should have open access to the Chief Compliance Officer.

One discipline that can drive board effectiveness in collaborating with management involves information reporting and focus. Today, we see many organizations working overtime to capture more compliance and risk information than they'll ever use. So when board members ask "what information is really needed," they could be providing an invaluable service to the rest of the organization, giving leaders the incentives they need to focus their efforts where it really counts. Information itself is never the goal. It's just the means to an insight.

"Sometimes doing your job as a board member is making sure everyone is eating the broccoli."

Must-ask questions

- ☐ Where does the board's responsibility end and management's begin?
- ☐ What knowledge and experience does the board currently lack in order to understand and effectively oversee our compliance programs?
- ☐ What do regulators and other external stakeholders say about the role of the board in ethics and compliance issues?
- ☐ How can the board determine whether resources devoted to compliance programs are adequate and aligned with the organization's risk appetite?
- ☐ How do our board activities align with Federal Sentencing Guidelines?
- ☐ How are senior leaders accountable for fostering a culture of compliance in their performance goals? How are they performing?

Remediation

Any robust business continuity program must deal with compliance failure. But remediation is often handled on a reactive basis: A company faces a compliance failure and then works its way out of the hole. The real challenge is to identify and address problems before they grow into true compliance failures. That's a job requiring a willingness to dive in at the business process level, understand what is and isn't happening, and begin making changes. In that sense, remediation becomes less about responding at a time of acute need and more about planning and continuous improvement, which should lead to fewer acute needs in the long run.

A continuous improvement approach to compliance is likely to require business leaders to fundamentally change their perspective on addressing compliance problems. For example, retooling and coordinating existing processes may help offer insights on challenges well before they strike. Internal audits, compliance isk assessments, hotlines, evaluations of internal controls and business processes – any of these activities could be instrumental in uncovering and addressing problems.

While a proactive approach sounds good in theory, the "squeaky wheel gets the grease" model is the one many leaders rely on amid a host of other issues vying for their attention. Meanwhile, many regulators (not to mention the Federal Sentencing Guidelines) recommend or require proactive measures. In that context, a proactive approach begins to sound like a better defensive strategy.

> "You want to look into the whites of the eyes of the people responsible for making sure problems are resolved."

Must-ask questions

- ☐ What is our process for remediating known compliance breakdowns? Who owns it?
- ☐ Which mechanisms are in place to help ensure that corrective action takes place?
- ☐ What escalation protocols have we developed in case our efforts begin to fall behind schedule?
- ☐ How are we learning from failure? How are we determining whether a specific failure was the result of a systemic problem?
- ☐ How are we identifying opportunities for continuous improvement when we conduct internal audits? What about compliance risk assessments? Evaluations of internal controls and business processes?
- ☐ How are we documenting the continuous improvement actions we're taking?
- ☐ What are the key performance indicators of successful remediation and continuous improvement?

Evaluation

Risk assessment

Ask a room full of senior executives or board members how their organizations handle compliance risk, and you're likely to hear a lot about how great their risk assessment programs are. But what about their *compliance* risk assessments? A risk assessment can cover a wide variety of issues, including compliance. But it can also give leaders a false sense of confidence, especially when it comes to compliance. A general, noncompliance-focused risk assessment is unlikely to deliver the information needed to fully understand and head off compliance risks.

It's safe to say we don't know what we don't know. That can be a big problem when the people conducting assessments at the business unit level have an overly narrow view of what constitutes a risk. Multiply that scenario by all the individual parts of an organization, and it can add up to an even bigger problem. In too many cases, no one is challenging these assessments. And so the cycle continues.

So how can leaders be confident that they have smart answers to the tough questions about compliance risk assessments? Developing a risk register can be a great way to start. This catalog of existing and potential *compliance* risks specific to the organization can ultimately serve as a framework for understanding and prioritizing risk at every level.

> "Without an enterprise-level view of assessments, we run the risk of being detached from the reality of our compliance environment."

Must-ask questions

- ☐ Why do you have confidence in what you're reporting now?
- ☐ Why were we wrong last time?
- ☐ How do you know you're assessing the right compliance risks?
- ☐ When was the last time anyone challenged the scope, approach, outcome, or results of an assessment?
- ☐ How do assessments match up with the issues management is tracking?
- ☐ How does our compliance risk assessment feed into enterprise risk management (ERM) assessments? Growth and M&A risk assessments? Internal audits? External audits? Do we define ERM somewhere?

Return on investment

Given the business environment today, it's no surprise that many organizations are pouring significant and increasing resources into compliance initiatives. Board members and senior executives are already asking what they've gained from all that effort and expense – and whether anyone is making sure those investments are being managed at the enterprise level.

There is at least one easy measure of the value that compliance efforts deliver back to the organization: avoidance or reduction of penalties. But a leading compliance operation recognizes the need to establish and monitor key performance indicators (KPIs) and key risk indicators (KRIs) for a more nuanced look at ROI. In fact, avoided or reduced penalties may be the least significant measure of all. So what else is there?

Reputation, for one. Companies that fall out of compliance can quickly encounter a public chorus of media and consumer critics bent on inflicting reputational damage that can take years to repair. Compliance failures can even trigger automatic removal from "preferred vendor" lists and the immediate loss of business because of partners' own risk guidelines.

To determine ROI, you first have to know how much has been invested or what is being gained. While it may not be realistic today to achieve a perfect view of your organization's compliance investments or returns, establishing the scope of compliance is a good place to start. Next, gain agreement on the KPIs and KRIs you should have in place to track ROI. Culture is the key to ensuring that the organization sustains its focus on ROI and responds appropriately over the long term.

Must-ask questions

- ☐ If we suddenly decided to invest nothing in compliance, what would happen?
- ☐ How have we linked our compliance efforts to safeguarding and building shareholder value, reputation, and assets?
- ☐ What are we doing to balance the requirement of compliance with the cost of complying – and the potential value we could realize as a result of having the right approach in place?
- ☐ Is there any inherent value of compliance to our organization beyond penalty avoidance? If so, what is it?
- ☐ Which KPIs and KRIs are our competitors reporting?
- ☐ How are we measuring the cost and value of compliance in our business? And how are we communicating the results to internal and external stakeholders?
- ☐ What could we change tomorrow to either reduce the cost of our compliance efforts or increase their value? Can we do both?

Monitoring

In theory, senior executives and board members have access to insights drawn from an unprecedented volume of information related to compliance risk, an amount that continues to grow every year. But as other parts of the business have already discovered, more information doesn't necessarily mean more insight.

In fact, more information often just introduces more questions: *Are we capturing the right data? How do we access it? Do we understand it? Does it align with the drivers of our compliance risks? What don't we know that we may not even be pursuing?* Many leaders say they're presented with more information than in the past but may be in no better position to act on it than before. Often, they're being presented with too much information. This is likely the result of a larger shift underway throughout the business: Business leaders are struggling under the weight of a growing emphasis on analytics and data-driven decisions.

Perhaps the most important question is really "how can we monitor what really matters?" Yes, monitoring can help uncover instances in which, for example, tax compliance has gone awry. But just as important, monitoring can be used to examine entire compliance processes as part of a continuous improvement effort. It can help detect emerging trends associated with key risk and performance indicators that are directly related to compliance; for example, imagine tapping external data sources such as blogs to better understand compliance issues in specific geographies in which your organization operates.

"We had way more information than was necessary, and no road map. That was a problem."

Must-ask questions

- ☐ How do we know we're getting the right information?
- ☐ Where is it coming from? Are HR, risk, compliance, finance and core systems providing information?
- ☐ How are we monitoring changes in the business and their impact on compliance risk?
- ☐ How is this information being combined with other data that drives compliance risk, from external and geopolitical data to other internal sources?
- ☐ Are we interpreting this information correctly? What other explanations were considered?
- ☐ How do our monitoring approaches and capabilities differ from those we used to have in place?
- ☐ When was the last time we changed our approach to compliance because of something we discovered in our data?
- ☐ What are our KPIs and KRIs? How do we know?

Target: Compliance culture

In this book, we've presented the key components of a leading enterprise compliance function. While it's tempting to focus on these individual parts, don't lose sight of the big picture. In the end, fully embracing all of them should result in a true cultural shift – one in which compliance is not just another box in need of checking but is simply part of how business gets done.

Just as important, these components contribute to the sustainability of a leading compliance program. It's one thing for an organization to hit its compliance milestones for a year or two. But what happens in the fifth year, or the tenth? Program sustainability plays a key role in ensuring that compliance investments continue to benefit the organization and pay off over the long haul.

Is it worth it? Today, Risk Intelligent compliance is slowly but surely moving into the category of "competitive advantage" as the global regulatory environment becomes even more complex. Those who can master the compliance aspect of their business strategy and give their people ample incentive to do the right thing may be better positioned to break away from the pack. And that's always worth it.

Talk to us

We look forward to hearing from you and learning what you think about the ideas presented in this book. Please contact us at **enterprisecompliance@deloitte.com.**