

# COMPLIANCE INSIGHTS

## An Open Letter to CEOs and Board Members: In Support of the Compliance Function<sup>1</sup>

*By Carol Beaumier and Bernadine Reese*

*We've all heard it said: "Tone at the top" is critical to the success of a compliance function, and financial institution regulators expect CEOs and boards of directors to foster a "culture of compliance" in the institutions they oversee. We'd expect most CEOs and boards, when questioned, to say this is their goal. But what happens when the CEO and the board – intentionally or unintentionally – send conflicting messages about the importance of compliance?*

At the risk (but not with the intent) of insulting CEOs and board members of financial institutions, we believe it's important to call out a problem that has faced the financial services industry for a long time: wavering support for the compliance function. No, it doesn't happen in all institutions, but it does happen in too many. And it needs to change for the good of the industry.


### Value of compliance

CEOs and boards intuitively know why compliance is important. The reasons are many: Compliance helps to establish trust with customers, ensuring they are treated fairly and consistently. Compliance mitigates risk, reduces the chances of financial penalties and/or

---

<sup>1</sup> The authors acknowledge that the format for this article is based on the "Dear CEO" letters that are issued by the UK's Financial Conduct Authority (FCA) and Prudential Regulation Authority (PRA) to raise awareness and highlight areas of concern regarding regulatory compliance and industry practices. We have borrowed this format because we believe this topic also merits the increased awareness of CEOs and board members.

significant remediation costs, and safeguards the institution's reputation and, in doing so, protects shareholders. Compliance serves as the conscience of the organisation, guiding it through the complex web of regulatory requirements, customer and shareholder expectations, and other competing demands. A strong compliance function provides a competitive edge.



Compliance serves as the conscience of the organisation, guiding it through the complex web of regulatory requirements, customer and shareholder expectations, and other competing demands.

And, if none of the above reasons is compelling enough, there's always this: Compliance is an obligation – the cost of being a regulated financial institution or offering regulated products and services. And in some jurisdictions, it's also important to remember that senior managers may be held personally accountable for compliance failures.

Still, not everyone sees value in compliance, at least not all the time. Compliance functions are still working to overcome negative perceptions of what they do: Compliance functions are the naysayers, the blockers that impede the business. Compliance is a cost centre. Compliance hands out punishment but never rewards. Compliance doesn't really understand the business. Compliance is always changing the rules. Compliance is inflexible. Compliance is rooted in the past and too slow to accommodate innovation. These negative perceptions are not always voiced, but they exist, nonetheless.

Finally, there are some institutions that still allow a false value proposition to persist. Those are the institutions where business leaders believe, "It's not my role to manage compliance; the compliance department does that for me."

## Mixed signals

Many of the same CEOs and boards that profess to be champions of compliance send mixed signals. Some of these are obvious. For example:

- Ramping compliance functions up and down depending on regulatory pressures;
- Not providing other support, such as technology investment, that compliance functions need to be effective;

- Pushing back on recommendations from Compliance itself, Internal Audit, regulators or other third parties on steps that should be taken to strengthen the compliance function;
- Allowing the business to focus on the letter (“Show me where it says that”) and not the spirit of the law; or
- Letting some businesses operate seemingly outside the rules with the belief that non-compliance is not an issue unless or until the regulators become aware of it.

Ramping the compliance function up and down is a particularly troubling signal but one that we have witnessed over and over again. While admittedly, institutions may find it necessary to add resources to deal with regulatory remediation, the decision to cut resources once the problem is fixed (or perceived to be fixed) often does not adequately consider whether the problem occurred in the first place because the compliance function was under-resourced and/or whether a smaller staff will be able to manage effectively new (often additive) processes that were deployed as a result of the remediation. Without this type of analysis, the result is often inevitable: The pre-existing issues recur or there is a break somewhere else because of the strain on compliance resources.



Research suggests that the cost of non-compliance in financial institutions is 2.7 times greater than what is spent on compliance.

Source: “Reducing the cost of compliance with cutting-edge compliance software like Copasys,” Coforge, 23 January 2023: [www.coforge.com/blog/bps-cost-of-compliance](http://www.coforge.com/blog/bps-cost-of-compliance).

Other signals may be more subtle but are nonetheless impactful. These may include not taking the time necessary to understand the breadth of compliance challenges facing the organisation and what needs to be done to manage them proactively; not treating the Chief Compliance Officer (CCO) as a business adviser and strategic partner who also has a vested interest in the institution’s success; and establishing compliance metrics that, while well-intended, may actually reinforce a “we” and “they” divide between the business and Compliance.

In most cases, the CEO and the board are not deliberately or consciously trying to undermine the compliance function.<sup>2</sup> They have myriad priorities to balance, and they make decisions they believe to be in the best interest of the institution at the time they make them. But these mixed signals influence how Compliance views leadership, as noted in a recent survey conducted by Corporate Compliance Insights (see table below). While this survey was not limited to financial services companies and was for the U.S. only, it nonetheless provides an interesting perspective on how Compliance officers may view leadership in their companies.

**What do Compliance officers think about leadership?<sup>3</sup>**

<b>Compliance officers who believe top leadership responds appropriately to communications from the compliance department</b>	<b>48%</b>
<b>Compliance officers who believe the organisation treats compliance as a priority</b>	<b>46%</b>
<b>Compliance officers who trust the leadership of their organisation</b>	<b>45%</b>
<b>Compliance officers who believe their organisation has a culture of compliance</b>	<b>44%</b>

Mixed signals also undercut the effectiveness of the compliance function, lead to more (and often repeat) compliance issues, and ultimately prompt compliance professionals to question whether they want to work for an institution that does not share their commitment – a question which is likely being asked by compliance professionals more frequently given the growing number of personal liability cases targeting compliance officers. In short, these mixed signals suggest that, despite what they may say, the CEO and the board may not truly appreciate the value of the compliance function.

We can illustrate some of these inconsistent actions by homing in on some of the current challenges facing compliance functions.

**Current compliance challenges**

In our recent edition of *Compliance Insights* reviewing 2024 [Top of Mind Compliance Issues](#), we identified a number of internal challenges that are compromising the effectiveness of some compliance functions. With the support of the CEO and the board and with some upfront

<sup>2</sup> A few examples of management of newer market entrants disparaging the value of compliance do come to mind.

<sup>3</sup> Source: *Compliance Officer Working Conditions, Stress & Mental Health*, Corporate Compliance Insights, 2022: [www.corporatecomplianceinsights.com/wp-content/uploads/2022/01/Compliance-Officer-Working-Conditions-Stress-and-Mental-Health.pdf](http://www.corporatecomplianceinsights.com/wp-content/uploads/2022/01/Compliance-Officer-Working-Conditions-Stress-and-Mental-Health.pdf).

investment that we think will have significant payback over time, Compliance can be better positioned to address these challenges. One of the internal challenges is resourcing, a topic covered in part in the previous section. The other internal challenges are horizon scanning, risk in change, digital risk, and compliance monitoring and assurance, all of which culminate in compliance risk assessment.

Developing an effective compliance risk assessment is foundational to building an effective compliance program. But compliance risk assessments in financial institutions are often incomplete and outdated the day they are published. The industry needs dynamic compliance risk assessments that leverage technology and analytics and that continually consider changes in the regulatory landscape, how the institution is managing program changes related both to new regulatory requirements and to the impact of technological innovation, and the results of compliance monitoring and assurance. But not all compliance functions have the tools they need to develop and maintain dynamic risk assessments that require all of these inputs.



According to Thomson Reuters, there are, on average, 220 new financial services regulatory updates every day. That is the equivalent of a new regulatory update issued every seven minutes.

Source: "Scanning the Regulatory Horizon," Mariano Giralt and Colin Ware, BNY Mellon, November 2020: [www.bnymellon.com/us/en/insights/all-insights/scanning-the-regulatory-horizon.html](http://www.bnymellon.com/us/en/insights/all-insights/scanning-the-regulatory-horizon.html).


In their role of providing oversight to the compliance function, the CEO and the board should be asking the CCO questions such as:

- How confident are you that the compliance risk assessment includes all the regulatory requirements that apply to the institution?
- How is our compliance risk trending?
- Are you comfortable that our processes for implementing new regulatory requirements are sound?
- Are the compliance monitoring and assurance programs robust enough to allow us to assert that all businesses are sufficiently focused on their compliance responsibilities and that our compliance controls are working, and/or to provide for early identification of problems?

- Are we being proactive enough in addressing our regulatory challenges and any identified gaps?
- Do you have a good understanding of how innovation such as generative AI is affecting our compliance program?
- Are there activities that Compliance performs manually that could be automated?
- What do you need from us to enhance and sustain the compliance program?

In answer to the questions about the current state of the compliance program, we would expect many CCOs would say, “We are doing the best we can with the resources we have available.” In response to the last question, the answer in many instances is likely to be “people and technology.”

Faced with a growing regulatory agenda, compliance teams need to be trained appropriately across a range of new compliance topics (e.g., ESG and operational resilience) and be able to understand and challenge the compliance implications of new technologies used across the business. This requires the recruitment of new skill sets (including data analytics, data scientists and AI) and training so that compliance professionals are equipped to be trusted advisers to the board, management and the business.



CEOs and boards may be surprised to learn how many activities are performed manually by Compliance.

CEOs and boards may be surprised to learn how many activities are performed manually by Compliance – among them, the compliance risk assessment documented in an Excel spreadsheet, the horizon scanning for new regulatory requirements that depends on one or more individuals following regulator websites and legal and consulting firm updates and informing the right people in the organisation about impending changes, and limited sample manual monitoring. There is technology that can help with these activities so that compliance professionals can focus more on interpreting and acting on the results and not on compiling information.

This is not to suggest that the CEO and the board should automatically agree to all the people and technology investments that Compliance requests — no responsible CEO or board would do that. But Compliance should at least be allowed to make its case, as any business function would, that investment would be in the best interest of the organisation.

We believe that CEOs and boards that support the compliance function journey with appropriate investment in people and technology will benefit from fewer regulatory incidents and issues, improved customer and market reputation, and better regulatory relationships. They will improve their ability to avoid costs of remediation, restitution to customers, enforcement actions and reputational damage, and they will have a more highly motivated compliance team to boot!

## Call to action

Unless the industry is prepared for history to keep repeating itself with troubling headlines about non-compliance, remediation costs that are multiples of the annual compliance budget and heightened regulatory scrutiny that often extends beyond the institution first identified with a problem, there need to be changes in the ways CEOs and boards oversee, interact with and support Compliance. The following are actions we believe CEOs and boards should take:

- **Define and continually reinforce the role of Compliance.** The CEO and the board should take every opportunity to make clear the role of Compliance and its importance to the strategy of the institution. Compliance is a partner, not an adversary. Compliance's responsibility is to protect the institution from actions that jeopardise its ability to achieve its strategic goals. That means sometimes, Compliance may need to say "no." But more often than not, given timely consultation, Compliance will be able to advise on the "right" way to do something.
- **Make accountability non-negotiable.** Holding individuals and teams accountable for compliance failures, regardless of their position within the organisation, reinforces the message that compliance is a priority.
- **Recognise contributions to the compliance effort.** Encourage employees to raise concerns or report potential compliance issues without fear of retaliation and recognise these individuals for being compliance champions. Celebrate the individual/team that went above and beyond to implement a new requirement. These actions provide positive reinforcement of the importance of compliance.
- **Hire and retain the best and the brightest to lead the compliance effort.** Hiring may be easy, but retention is not. The CCO needs to be viewed as a valued member of leadership, one who consistently has the same platform (including meaningful time on the board agenda) and

visibility that is given to the most successful business leader – not just when the institution is dealing with regulatory remediation but all the time. Also, make sure, by adding or reskilling as necessary, that Compliance has the right expertise to be successful in the current environment.

- **Set (high) expectations for the CCO.** Beyond being an expert on laws and regulations, the CCO, among other competencies, needs to understand the business, be knowledgeable about the impact of technology and innovation, be a master communicator and relationship builder who is able to convince (not order) people to do the right thing, and be bold enough to tell the CEO and the board what's not working and what's required to fix a problem.
- **Commit not to scale the compliance function up and down.** When a business unit does well, it is usually rewarded with more people and capital to grow. When Compliance does well, as evidenced by the lack of regulatory pressure, often the impulse is to reduce resources. That does not make sense if not supported by thoughtful analysis. It's the equivalent of cancelling your insurance and gambling that nothing will go wrong.
- **Invest in compliance.** Some of the funds the industry has historically spent on regulatory remediation need to be redirected to modernising the compliance function. Better use of technology and analytics by Compliance can provide better coverage of compliance activities and greater comfort that problems are being identified timely. It can also free up compliance personnel to focus on the most important issues.
- **Develop and implement meaningful metrics for measuring success of the compliance effort.** Rather than establishing separate compliance metrics for the business and the compliance function, link compliance objectives to business goals to reinforce the partnership that should exist. The CEO and the board can set examples by making compliance goals part of their annual scorecards and communicating to the organisation those goals and, periodically, the progress toward achieving them.
- **Actively endorse the compliance program.** Having the CEO or a board member introduce a compliance training session or participate in a compliance town hall meeting, if only to kick it off, are easy actions the CEO and the board can take to make their support visible.

The bottom line: Only when the CEO's and board's actions, and not just their words, are *intentional, consistent* and *unwavering* can there be a culture of compliance. The CEO and the board have an opportunity to set the right tone at the top by collaborating with Compliance as a value-added function that not only protects the institution from potentially significant fines and reputation damage, but also provides a competitive advantage in an increasingly complex regulatory landscape.

*The authors would like to thank Stephen Stachowicz, Anthony Gibbs and Hyung Kim for sharing their views on this topic.*



## About the authors

**Carol Beaumier** is a senior managing director in Protiviti's Risk and Compliance practice. Based in Washington, D.C., she has more than 30 years of experience in a wide range of regulatory issues across multiple industries. Before joining Protiviti, Beaumier was a partner in Arthur Andersen's Regulatory Risk Services practice and a managing director and founding partner of The Secura Group, where she headed the Risk Management practice. Before consulting, Beaumier spent 11 years with the U.S. Office of the Comptroller of the Currency (OCC), where she was an examiner with a focus on multinational and international banks. She also served as executive assistant to the comptroller, as a member of the OCC's senior management team and as liaison for the comptroller inside and outside of the agency. Beaumier is a frequent author and speaker on regulatory and other risk issues.

**Bernadine Reese** is a managing director in Protiviti's Risk and Compliance practice. Based in London, Reese joined Protiviti in 2007 from KPMG's Regulatory Services practice. Reese has more than 30 years' experience working with a variety of financial services clients to enhance their business performance by successfully implementing risk, compliance and governance change and optimising their risk and compliance arrangements. She is a Certified Climate Risk Professional.

## About Protiviti's Compliance Risk Management Practice

There's a better way to manage the burden of regulatory compliance. Imagine if functions were aligned to business objectives, processes were optimised, and procedures were automated and enabled by data and technology. Regulatory requirements would be met with efficiency. Controls become predictive instead of reactive. Employees derive more value from their roles. The business can take comfort that their reputation is protected, allowing for greater focus on growth and innovation.

Protiviti helps organisations integrate compliance into agile risk management teams, leverage analytics for forward-looking, predictive controls, apply regulatory compliance expertise and utilise automated workflow tools for more efficient remediation of compliance enforcement actions or issues, translate customer and compliance needs into design requirements for new products or services, and establish routines for monitoring regulatory compliance performance.

---

Protiviti ([www.protiviti.com](http://www.protiviti.com)) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independent and locally owned Member Firms provide clients with consulting and managed solutions in finance, technology, operations, data, analytics, digital, legal, HR, governance, risk and internal audit through our network of more than 85 offices in over 25 countries.

Named to the 2023 *Fortune* 100 Best Companies to Work For® list, Protiviti has served more than 80 percent of *Fortune* 100 and nearly 80 percent of *Fortune* 500 companies. The firm also works with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.