Building Resilience to Compliance Ecosystem[1]

If anyone here believes that human capital is the most valuable asset of a bank, compliance could naturally follow as the best investment option. In banking, compliance is not a matter of choice but the very foundation; ignoring compliance is not merely a lapse but a malpractice. That about encapsulates how a Chief Compliance Officer (CCO) in a bank needs to be valued. Before you start feeling a bit flattered warily, let me add that the reference is to the challenges of earning and assuming that big value title. It can happen by not just reinforcing the existing compliance playbook, but by dynamizing it enough for right alignment with the changing business landscapes and regulatory ecosystem, to supplement. The 'whats' alone of a compliance job is not adequate capital for a Compliance Officer anymore in order to understand the expectation and challenges. The 'whys' and 'hows' assume more equal importance, particularly when there is a trend away from the prescriptive regulatory regimes, accompanied by broadening of regulatory perimeters, which may appear as disruptive to the unprepared. Going by some developments in the industry lately, building a compliance program that can hold off stress, learn from failures, be able to effectively anticipate, adapt and recover from disruption or changes, while not failing on its compliance obligation become the top *desiderata* from a CCO. On ground, these attributes can not to be limited to the domain of the CCO alone but to extend much beyond. That, in short, is what can be termed as building resilience to the compliance ecosystem. It is about moving beyond simply meeting regulatory requirements to building a robust system that can withstand challenges in a dynamic environment.

Positing a Resilient Compliance Function

2. Regulatory discourses in India often quote audit, risk management and compliance functions as the trifecta of internal assurance. Audit and risk management, by their very nature, take a backward- and forward-looking view of the objects of their assurance, respectively. On the other hand, compliance necessitates a multi-sided

[1] Keynote Address by Jayant Kumar Dash, Executive Director, Reserve Bank of India at Conference on Chief Compliance Officers: Expectations and Challenges on May 20-21, 2025 in Mumbai

approach embodying both retrospective analysis (back-ward looking view) and proactive planning (forward view) displaying higher degree of versatility.

3. To understand why the compliance function cannot be a mechanistic script, reference to one of the classic regulatory approaches called 'harms approach' may be helpful[i]. In today's context, harms would mean the complex and multi-dimensional risks that can be created by the banking and non-banking regulated sectors. This approach acknowledges that while existing compliance programs and processes can be beneficial, they may not always be sufficient to address all potential risks, particularly in complex or evolving situations. In terms of the approach, regulators would shift their priority from being focused on mere 'illegal' things (i.e non-compliant matters) to 'harmful' (risky matters) things that could be both illegal and legal (i.e either non-compliant or technically compliant) by implementing tailored interventions using full range of tools at their disposal. The author of the approach (Prof. Malcolm Sparrow) further talks about "regulatory pendulum" which swing from trusting and cooperative postures back to adversarial enforcement-centric strategies after negative events. That leads one to a sphere which is often termed as 'beyond compliance' that the CCOs need to be cognizant of, in the context of regulatory risk. Besides, the accountability aspects of the assurance function unmissably crop up in various episodes of deviant conduct, even without an individual accountability regime in India, unlike in some other jurisdictions. In an industry with the reputation of being one of the most-regulated, the question of compliance cannot be taken lightly without considering possible Newtonian consequences.

4. Any assurance function would essentially have three participants i.e the institution, the beneficiaries and the assurance-provider with a hallmark of independence. While the primary beneficiaries of robust assurance function are the institution and its stakeholders in various scale, compliance function stands out in terms of its direct intersection with the regulators, straddling all other assurance and business functions. Compliance function operates over two levels viz. (i) external rules including regulations and (ii) internal systems of controls laid down to comply with externally imposed rules. It is difficult to come across risk events in a bank or NBFC which does not have a close or distant compliance linkage.

5. Digital transformation has somewhat compounded the architectural complexity of banks and large NBFCs. Regulations have tended to multiply globally and nationally, not only for addressing these complexities, but also to keep pace with increasing stakeholder expectations for safe and secure operations. Thus, managing compliance risk becomes, not just a moving target, but rather presents multiple targets that snowball as the business and technology expand. Continuous evolving of laws, regulations, policies and standards across the spectrum often represent one of the biggest overall enterprise risks to address. To manage such shifting scenarios and to adapt, it is essential that the compliance function in banks and NBFCs build adequate vision, strategies and innovative capabilities for resilience.

Traditional Compliance Risk Assessment Approach

6. Being majorly a function of external rules & regulations, the inherent compliance risk becomes vertically proportional to the level of compliance exposure in terms of products, services, activities, assets (including digital assets) along with their complexity. Further, the inherent compliance risk would be horizontally proportional to the volume of such activities. The gaps in internal compliance structures such as policies, standards, and procedures to meet the regulatory compliance in letter and intents quantifies for the residual compliance risk. A static Compliance Risk Assessment Framework, a basic instrument of quantifying compliance risk, could typically consist of a (i) Regulation Matrix and (ii) Compliance Risk Analysis. The matrix inventorizes all the laws, regulations, standards, other norms etc. and map them to relevant business units, products or services. Quantification of compliance risk also bakes in the criticality of the inventory reckoned on a risk-prioritized basis. The Compliance Risk Analysis imputes inherent compliance risk to each of the inventory and arrives at the residual risk level by analysing the respective control methods for the identified risk(s). It also recommends methods to trim the unacceptable residual risks to an acceptable level. It is important to choose an appropriate scale to quantify the compliance risk beyond colour codes or qualitative scores. It needs no emphasis to understand that compliance risk assessment is not a one-time activity and needs to be carried out at regular intervals.

7. The above conventional approach to risk measurement would further tell us that Inherent Compliance Risk for an item of the inventory is Impact of the compliance

failure times its probability. Residual Compliance Risk is the Inherent Compliance Risk times the Control Effectiveness. Control Effectiveness is measured by Control Impact times the Control Ineffectiveness. However, in many cases, the CCOs use rather intuitive metrics as a proxy to a systematic analysis, to measure compliance risk or do not review or manage such metrics regularly for necessary adjustments / continuous improvements. Many times, the metrics are not appropriate and such practices tell upon the resilience quotient of the compliance programs and measurement of compliance risk.

Drivers of a Resilient Compliance Ecosystem

8. **Synthesizing rearward and forward views of compliance** is the fundamental plank for a resilient compliance ecosystem. The retrospective analysis encompasses understanding the historical compliance performance, identifying source causes for past deviations, learning from the mistakes and improving policies and procedures / training etc. This also amalgamates incidents involving peers, to an extent possible. A second element of proactive planning, on the other hand, could involve staying ahead of changes by monitoring and minding regulatory consultation processes, updates, industry trends and emerging technologies to realign compliance strategies. Anticipative assessment of potential impact of new regulations or changing market dynamics, particularly in consultative regime of regulation making, would help a bank/ NBFC develop strategies to minimize compliance risk, provided they are prepared for it. Anticipating future compliance needs can streamline or modularize the processes and resource allocation for a more effective and resilient compliance program.

9. **Compliance benchmarking** involves evaluating an RE's compliance program against industry standards, peer (or, prospective peers) institutions, and regulatory expectations to identify weaknesses, and areas for improvement. This process lends some degree of assurance about the relative degree of effectiveness, being well-versed and resilient to evolving risks and regulatory changes. It is vital for actualizing proportionate and innovative compliance solutions, meeting regulators' expectations, improving overall compliance posture and contributing to long-term success of a bank/ NBFC. The scope of compliance benchmarking stretches across policies and procedures, compliance risk management, reporting and monitoring of compliance performance, and resource allocation. Benchmarking methods adopted for such

exercise, as mentioned, typically cover peer reviews, industry surveys, global standards / best practices, regulatory audits, internal assessments. As a corollary, participation of CCOs in industry fora and regulatory interfaces and increased exposures to better practices make ample sense from benchmarking perspectives.

10. **Building a Culture of Compliance** may sound as another timeworn piece of advice. But nothing can be more appropriate factor for a resilient compliance program, when pitted against the definition[ii] of regulation. In the broadest sense, "regulation seeks to change behavior to produce desired outcomes" and we often relate behavior to culture of persons and communities. After all, compliance is the business of the business teams rather than that of the compliance functionaries alone. A culture of compliance must therefore be a sacrosanct part of corporate culture. This ingrains compliance into day-to-day workflows and sets the bedrock for employee behavior, insofar as compliance is concerned, across a bank or an NBFC. An internalised compliance culture, where employees assimilate their responsibilities and are empowered to raise issues, is essential for building compliance resilience. A compliance culture, where ethical behavior and compliance are valued and practiced, significantly enhances compliance resilience. It fosters trust, minimizes risks, and empowers employees to make ethical decisions, leading to a more agile and resilient business. When compliance, seen in a context, operates in the 'legal but harmful' part of the Venn diagram under 'harms approach' to regulation, that becomes start of a spiral of newer complications. Thus, the basic levels of a culture of compliance would include (i) the letter of the law/regulation, being the sacred minimum; (ii) the spirit of the law/ regulation, which is an expansion of the intents, and (iii) adoption of leading / best practices in the industry, being proactive. The main substructures on which this culture can thrive could include understanding of right regulatory practices, regulatory training on an ongoing basis, clear messaging around employee conduct, a consequence framework, technology for improved compliance governance, and an effective incident reporting & response system.

11. **Compliance Stress Testing** is a form of stress testing that specifically evaluates a bank's ability to adhere to regulatory requirements and internal policies under unexpected adverse or extreme conditions. Given that most other typical stress testing have a compliance angle, compliance stress testing is an important aspect of risk

management, helping identify potential weaknesses in compliance procedures and control processes. This involves duplicating potential real-world scenarios of varying severity, testing processes and controls, and evaluating potential consequences. It can be done through scenario-based stress tests, where specific events are constructed, or by analyzing historical data to identify potential unaddressed vulnerabilities. Illustratively, simulating a sudden surge in regulatory scrutiny intensity on certain practices or business; or a major market event to see how increased regulatory reporting requirements or potential breaches of regulatory limits can be handled. It could also involve simulating a load on transaction processing calls, disruption to third party services supply chains / platforms, cybersecurity threats, or changes in legal regulations to assess compliance with evolving laws. Developing appropriate and commensurate mitigation strategies to reinforce compliance programs and improve resilience would be the next stage, after due analysis of possible impacts of compliance failure.

12. **Leveraging Technology** for a resilient compliance ecosystem is the easiest factor to name but when designed with a long-term view, it can play the most crucial role. Using technology to automate standard tasks, streamlining compliance processes, providing transparency or traceability, enabling continuous auditing/monitoring, and facilitating recovery can hugely build up compliance resilience. Further, digital solutions can ensure consistent application of internal policies and procedures, and a good version control system can maintain a clear audit trail by tracking changes. Technology like AI/ML helps REs identify, extract, and classify relevant regulatory obligations, accelerating the regulatory change management process. AI/ML solutions for detecting potential compliance risks and implementing preventive measures to help a predictive compliance risk management approach could be a reality soon. Technology can also smoothen communication and training on new regulatory needs, ensuring that employees understand their role / responsibilities and can adapt to changes quickly. Finally, it is technology which alone can engage with the most conspicuously forbidding cyber security defences, data encryption and access control, incident response and crisis management.

Cost Benefit Conundrum

13. A less-addressed subject, compliance may still be considered as a cost to the cost-conscious banks / NBFCs; but it certainly is not a discretionary cost anymore, in light of heightened enforcement actions for non-compliance globally. More mature entities count in a resilient compliance program as a prized business enabler contributing to their differentiated positioning, profitability, growth and long term sustainability. This entire transformation cycle has happens by focussing on pivotal realignment with technology levers, and use of data / data-analytics; thus transfiguring compliance function from a cost centre into a strategic advantage. A compliance budget can also be a tool to assess the costs and benefits of adherence to organizational compliance goals.

14. While undertaking any cost benefit analysis (CBA) of a compliance program, apart from direct and indirect costs, REs need to typically count in opportunity costs and long term costs such as dented reputation / stakeholders' trust for compliance failures. On the benefit side, the factors that count may include notional cost savings, enhanced efficiency & productivity, benefits from risk mitigation, improved reputation & trust, apart from new business opportunities that open up. For a financial service firm, a well-structured CBA can adapt traditional tools such as Net Present Value (NPV) or Internal Rate of Return (IRR) to arrive at some objective outcome, though not easily. The results can be supplemented by sensitivity analysis to assess the impact of uncertainty on the sides of costs as well as benefits. A break-even analysis can also be adopted as a theoretical approach to arrive at the 'just cost' of compliance. However, maintaining an 'efficient frontier' of risk and compliance is complex customer under dynamic situations, as discount factors and timeframes further add to the complexities.

15. On the other side of regulatee, regulatory impact analysis (RIA) or cost & benefit analysis (CBA) by regulators has moved from the back-rooms to the forefront of designing and implementing regulations, with consultative processes thrown in for a right-touch approach. Some of the recent initiatives by RBI in this direction is known to the audience. REs cannot effectively patriciate in this open regulatory process unless they are familiar with the context of compliance and methods for undertaking CBA for themselves as well as in the context of the system. Hence, being part of the

regulation designing is a new mantle that the CCOs should be ready to were when demand arises.

16. Theory of convenience, when applied to cases of non-compliance by banks / NBFCs, could sometimes explain proliferation or increasing complexity of regulation to address a fewer deviants than a larger compliant population. When this regulation imposed cost is targeted to be avoided, the cost of smart deviations (i.e 'compliant but harmful' under harms approach) would continue to hang heavier on the entities for adopting a convenience or utilitarian approach to compliance assurance. Operating in regulatory grey zones would always have the risk of facing matching enforcement tools. Hence, 'beyond compliance' approach is often considered as the right approach to operate under a growing regulated financial services sectors.

Ecosystem Approach

17. An "ecosystem approach" to a compliance resilience underlines a non-segregated and holistic view of risk management, and viewing compliance as a complex network of interrelated elements, rather than siloed functions. This approach recognizes how different compliance components interact and influence each other to achieve overall risk mitigation and regulatory adherence. It bounds all the key stakeholders, such as employees, board members, and external parties, in the development and implementation of compliance programs. Collaboration and communication across different functions to ensure a consistent and coordinated approach, thus, becomes a *sine qua non*. Data analytics and information systems for monitoring multi-disciplinary compliance activities, identifying trends, and inputs for decision-making are salient attributes of such a program. This approach recognises the constantly evolving nature of compliance landscape for which adaptive and flexible exercises ensure continued effectiveness. Proactive risk identification and mitigation strategies to prevent compliance failure or landing in grey zones on unvalidated assumptions are key levers of a resilient compliance program.

18. Some among you may have been a studious observer of updation of the popular term "three lines of defence" to "three lines" by its author i.e the Institute of Internal Auditors (IIA) in July 2020. This was done with the stated objectives to "*better identify*

and structure interactions and responsibilities of key players toward achieving more effective alignment, collaboration, accountability and, ultimately, objectives." Thus, a reactive approach to risk management through three independent barriers "defending" the business been replaced by six key principles to nurture a collaborative approach. The inter-line collaboration, as against an independent existence in its former avtar, point to an joined-up approach to working. The individual employees are put in a position to take a holistic view of affairs rather than their own role, under the new model. While the documented concept may not have given due importance to compliance function explicitly, unlike in the older version, the keystone character of compliance continues as a part of overall governance structure. That is a clear indicator towards an ecosystem approach to a resilient compliance rather than an traffic island approach for compliance functionaries.

19. From a more low-down perspective, the availability of compliance modules in different rule engines in various business applications and embedding of compliance rails in designing of any new products and services can help to a great degree. The CCOs may keep in mind the 'beyond compliance' buffer approach is adoptyed while developing both the applications as well as the modules – a concept often referred to as "compliance by design". Tools that would enable automated compliance reporting and documentation need to said bundled as well. In a sense, to borrow a covid-time word, ecosystem approach to compliance is like 'herd immunity' where spread of the virus of non-compliance in an environment of compliance.

20. The next related low-down of compliance concerns hovers over 'application sprawl' i.e a sprawling digital application environment, with sparse involvement from inhouse technology teams of an RE. This greatly expands and complicate the resilience risk surface. Experts suggest 'composability' as a possible approach to the solution. Composability means designing the applications as "packaged business capabilities" (PBC), rather than separate or siloed products used to address a single business need. Such applications can be designed, assembled and integrated to provide tailored solutions, cutting down the sprawl and reducing resilience risks. In the context of application compliance, deploying applications from reusable, independent components that can be combined and re-configured to meet specific compliance requirements. This strategy allows for quicker adaptation to regulatory changes and

reduces the risks of errors compared to monolithic or highly integrated systems. Hence, the key considerations in design of application architecture should weigh in features such as interoperability, reusability, maintainability and testability for an agile turn-around for changes with less dependence on application development activities.

Near Fronts for Compliance Resilience

21. When a risk consistently appears as "emerging" year after year, oftentimes risk managers lose their initial gravitas and focus. In case of newer technology, they pass through different stages of maturity, adoption and social application, styled as hype cycle. However, when it comes to risk, such elongated stay may actually suggest a long-term, ongoing trend or a slow-developing storm that is not yet fully landed but has the potential for significant impact in the future. This indicates that such risks are not sudden shocks but rather gradual shifts in the risk landscape that requires continuous monitoring and proactive adaptation. As I see, there is a bunch of such risks lined up for detailed discussion during this conference. However, if one analyses a few recent episodes of compliance failure with consequences, possibly the phrase “Elementary, my dear Mr Watson” would cross one’s mind, those not necessarily being from any emerging risk list. Nonetheless, it would be apt to pick up a few of fronts where compliance preparedness / resilience would be an essential virtue.

21.1 **Use of Artificial Intelligence / Machine Learning (AI/ML)** is coming up as the topmost challenge to compliance for banks in most global surveys. In India, RBI surveys indicate its adoption to be very nascent with a few large banks / NBFCs is taking small leaps in less-critical use cases. It means that this is the right time to understand and build compliance resilience to such developments before they are mainstreamed. The rise of AI introduces concomitant compliance risks, with opportunities. CCOs will need to understand the ethical implications of AI, ensure that such systems are compliant with relevant regulations (like data privacy), and leverage AI for automation to streamline compliance processes. Better understanding of model risk management (MRM) would be helpful while bringing more AI/ML tools to working of banks / NBFCs. The compliance team need to be aware of invisible but serious conduct risks found embedded in certain other non-financial apps and such practices be prevented in financial service apps.

21.2 **Third Party Risk Management** (TPRM) is a fraught subject with webs of compliance implications in various shades of grey, particularly when most such third party service providers (TPSPs) are Tech or FinTech centric entities with little compliance exposures. The perceived borders between functioning of the regulated entity and their unregulated partners is often illusory in a borderless invisible cyber environment. The most tell-tale description of their relationship with banks data is often conveyed by the term 'a distinction, without difference'. There is move in a few jurisdictions or domains to bring such critical service providers under the ambit of direct regulation. However, the principle used in case of RBI is to address it indirectly through the governance mechanism of the regulated entities. To simplify the context, it is fair to say that FinTechs or other Tech partners are as responsible for compliance as the banks or NBFCs are, as the REs stand to be vicariously accountable. The compliance function of the regulated entity face challenges in ensuring it through business units or undertake compliance tests. Embracing of open banking / co-lending and fostering an ecosystem banking model, banks leverage external expertise, fast-track innovation, and explore new business models but increase their compliance risk exposure.

21.3 Evolving developments in **Climate Risk** management by banks / NBFCs may need paradigm shifts in compliance with potential need for additional data as well as granularity of existing data, reporting obligations and new instruments as the regulatory designs evolve in India. Anticipative preparedness for such scenarios is not difficult as access to various global resources and Indian approach are available to a large extent.

21.4 **Data Privacy and Cyber Security** continues to be the most daunting challenge, equally to the risk managers as well as compliance functionaries. Banks / NBFCs face progressively sophisticated cyber threats, in the forms of ransomware, phishing attacks, and large-scale data breaches etc. Deployment of AI-driven detection and response systems offering real-time monitoring and advanced protection mechanisms may offer some mitigation of such risks of REs. Robust data governance policies with full capability to comply with upcoming data privacy notifications, further strengthening security frameworks could work as good support for ensuring compliance. However, investment in cybersecurity defences by REs is not matched by third-party vendors

relied upon, creating additional vulnerabilities. Bank/ NBFC customers are comparing their banking experiences to the digital experiences they have in other spaces, thus raising the expectation bars for the REs. Meeting these expectations while maintaining security and trust and above all, being compliant is not an easy walk.

21.5 Banking regulatory objectives can be broadly categorized into three key areas: prudential, **conduct,** and market failure prevention. The latter two can be bracketed under consumer conduct and market conduct respectively. These are areas where compliance functions need to be more sensitive even when there may be no technical violation. Certain uncompensated risks may create narratives that tend to create a downward spiral from many important stakeholders. There have been exemplary cases of such instances in Indian environment itself where non-market risk management failure has led to cases of falls. In most such cases, the responsibility of compliance function in terms of omission or commission is inescapable.

Conclusion

22. The system of a 'Compliance Officer' in banks was introduced by RBI way back in 1992 and that for NBFCs rather recently. However, the compliance function continues to be still in a catch-up mode rather than levelling up, as expected by the regulators. In the year 2025, compliance resilience is confronting a confluence of factors such as hyped technological advancements, fast-evolving regulatory landscapes, and increased geoeconomic fluidities. These challenges will require banks and NBFCs to adapt their strategies, technologies, and resource pools to maintain operational stability, and withstand disruptions – equivalent of a difficult *bhavai* performance, neither missing the steps nor the balancing the pot on head while wearing a beatific smile. Hence, concepts like resilient compliance systems is gaining ground. As we have seen recently in more critical strategic matters, there is no alternative to well-preparedness and innovative plans to win. In order to spearhead this mission of compliance resilience embedded in all other resilience subjects, the CCOs are best placed leaders to be at the helms.

23. Building a resilient compliance system for banks involves a holistic approach i.e an ecosystem accroach for integrating resilience thinking into all aspects of operations including TPSPs, risk management, business continuity, and technology, as well as

nurturing a collaborative culture and kaizen. This warrants a comprehensive approach that addresses both internal and external factors, and leverages technology to automate and enhance monitoring as well as response and consequences.

I compliment CAFRAL for organising this program wish this two days conference some very useful and interactive deliberations with takeaways of some value.

Thank you.

---

[i] The Character of Harms: Operational Challenges in Control by Malcolm K. Sparrow

[ii] Cary Coglianese," Measuring Regulatory Performance: Evaluating the impact of regulation and regulatory policy", OECD