PERSPECTIVE

Regulatory compliance management in banks: Challenges and complexities

Infosys
be more

In recent years, managing regulatory compliance has become enormously challenging for banks, what with the incessant onslaught of new or revised regulations and the aggressive `take no prisoners' approach of many regulators across the globe. Over the past few years, the volume of regulations has risen dramatically. Nonetheless, new regulatory mandates continue unabated. It is estimated that by 2020, global banks would be required to comply with over 120,000 pages of regulations. Larger multinational banks have to comply with enormous complex national and international regulations that in some cases get even more complicated due to individual regulators' discretion and judgment. Not just the larger banks, smaller ones, too, are required to fulfill thousands of regulatory obligations. Many new regulations are broad and still evolving and yet, have stringent implementation timelines mandated. The two headline news below emphasize the volatility vis-à-vis bank regulations.

Recently, it was announced that the European Union (EU) is further tightening its money laundering controls. The European Commission is recommending a number of measures such as closer monitoring of cash transactions and bitcoin; national payment account registers creation, etc. The Fourth Anti-Money Laundering Directive (AMLD) that was introduced in 2015 is expected to undergo many more amendments in the coming months.

Pressure has been building on the European Commission to delay the MiFID II reforms implementation date by a year, as the concerned financial institutions struggle to enable their IT systems to meet the planned 2017 timetable.

Not surprisingly, banks today spend heavily to ensure compliance. For example, Britain's largest banks today spend ~£660 million a year on AML compliance alone. In spite of such a heavy outlay, banks are not unscathed from the regulators' ire. Some estimate that in 2014 alone, European and US banks had to pay ~US$65 billion in regulatory fines and penalties – a whopping 40% increase from the previous year. 2013 held the highest record, until then! In 2013, JPMorgan Chase had to pay US$13 billion towards regulatory settlements. In 2014, Citi paid US$7 billion and Bank of America US$16.7 billion. Further, banks are today subjected to full public announcements of their regulatory noncompliance. Even the slightest suggestion of noncompliance attracts headline news and therefore, reputational damage.

Alas, amidst such a challenging environment, most banks' current compliance management approaches fall short. Banks' outmoded approaches are beset with myriad issues, which make compliance enormously challenging. Here's a list of key concerns with the banks' current compliance management approaches.

Structure

- Banks' compliance efforts are narrowly focused on a centralized governance, risk and compliance (GRC) function. As a result, banks have been unable to build new competencies required for countering emerging compliance risks. For e.g., many banks' customer experience programs are disconnected from their compliance risk programs, even as customer experience aspects significantly impact compliance risks today.

- GRC functions of banks have constricted interpretation of compliance risk, which is detached from the banks' broader operational and business risks. Compliance management activities lack integration with the banks' broader risk management processes.

- Compliance has evolved to encompass new risk sources such as channel, product, customer, and operations. It is embedded across the banks' business activities and has become much more complex and intertwined. However, the banks' GRC function has not evolved their strategy to address compliance risks emanating from these newer risk sources.

- Lack of end-to-end and bank-wide compliance management framework to seamlessly integrate myriad regulatory mandates and make it easily accessible and understandable for all concerned stakeholders.

- Compliance function is still focused on 'high risk to the bank's bottom line' businesses areas. In many banks, regulations are usually addressed by the lines of business (LOBs) `that are the most affected'. For e.g., in some banks for FATCA compliance, tax division took the charge. This results in siloed understanding and implementation of the regulation.

- The compliance responsibilities for a centralized GRC function versus that of the LOBs are not clearly defined. There is inconsistency in compliance and risk functions' organization structures across LoBs. This creates enormous challenges in designing and implementing appropriate risk governance, assessment, monitoring, and testing approaches across LoBs.

Suboptimal strategy

- Compliance management is not inextricably linked to the banks' business decision-making process. So, instead of using a `preventive defense' method, a `compliance sign-off (checking boxes)' approach is followed. Compliance is treated as a necessary evil and an after-the-fact activity – even though most of the banking activities today are conducted in real time.

- GRC programs are managed in a haphazard and uncoordinated manner, resulting in inconsistent and half-baked implementations. Banks' risk and compliance management solutions address risks in silos, for e.g., only financial risk, operational risk, or SOX compliance.

- Banks run a parallel risk and compliance initiative. Risk and compliance activities are managed in silos by separate departments of the bank, use different and disparate data sets, and varying processes for risk reporting, assessment, and testing across LoBs.

Inferior approach

- Banks' compliance management functions face huge shortage of skilled personnel, for e.g., AML compliance-related professionals in the UK, default servicing legal experts in the US.

- Traditionally, a bank's compliance staff operated mostly in the advisory capacity and did not have to work on actual risk identification / management. With the changed regulatory environment and complexities, the staff has a tough time in reinventing themselves. They lack the understanding of business operations, the underlying compliance, and other risk imperatives. And yet, banks have failed to come up with a coherent and effective strategy to optimally up-skill their staff.

- Banks have been hiring thousands of new regulatory compliance specialists, without putting a robust staffing plan in place. This has further intensified the battle for scarce talent and associated costs. For example, by the end of 2014, Citigroup had ~30,000 of its staff engaged in the regulatory compliance aspects – an increase by around one-thirds in just three years. Similarly, JPMorgan Chase expanded its risk control function staff by ~30%.

Deficient staffing and skills

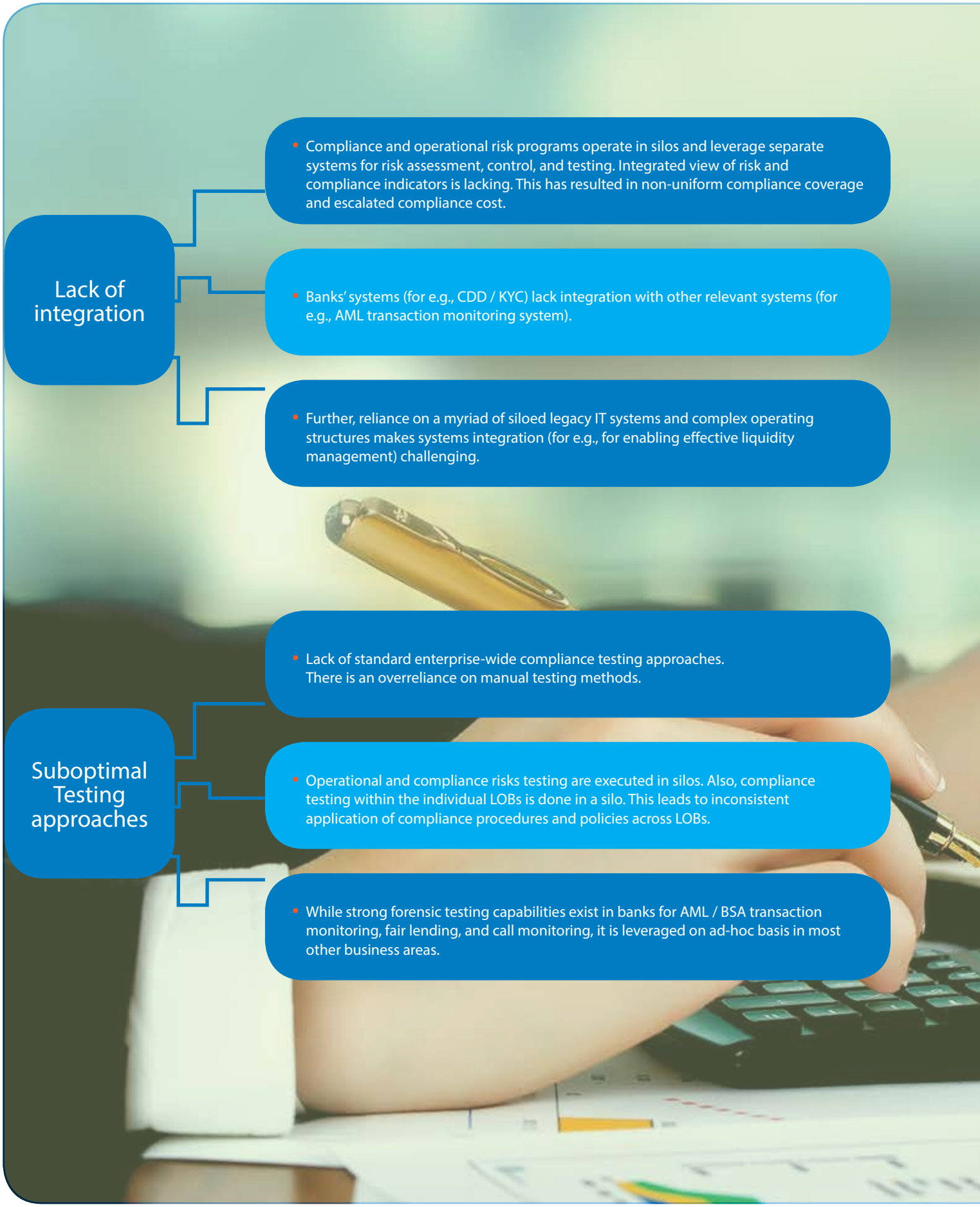
Technology

Suboptimal IT strategy

- Compliance IT implementation efforts focus solely on the initial compliance mandates and little or no attention is paid on the sustainability aspects. This leads to non-standard `quick fixes' that increase the future complexity and reduce scalability.
- Banks have taken a tactical workaround approach, rather than a holistic and strategic approach towards meeting compliance requirements. This leads to inherited `technical debt, for the future and at that point in time, remediation becomes extremely costly and challenging.
- As new regulations were introduced over the years, banks simply developed / purchased point solutions for managing specific regulatory mandates. This has led to, over the years, creation of duplicate systems, data stores, documentation, and processes.

Inadequate automation

- Lack of automated compliance management system. There is heavy reliance on labor-intensive, slow and error-prone manual files, hard copies, and Excel spread sheets, which are often stored in different departments of the bank.
- Banks' compliance processes (for e.g., customer due-diligence / KYC) lack standardization and automation (for e.g., information collection and manual onboarding). This results in significant process slow-downs, lost fee income opportunities, and poor client satisfaction. There is heavy usage of semi-automated and unsophisticated tools.
- With myriad digital channels (websites, social media, mobile apps, search engines, marketplaces, and more), banks lack the technology capabilities to effectively track all the channels to identify compliance policy violations and risk events



Lack of integration

- Compliance and operational risk programs operate in silos and leverage separate systems for risk assessment, control, and testing. Integrated view of risk and compliance indicators is lacking. This has resulted in non-uniform compliance coverage and escalated compliance cost.
- Banks' systems (for e.g., CDD / KYC) lack integration with other relevant systems (for e.g., AML transaction monitoring system).
- Further, reliance on a myriad of siloed legacy IT systems and complex operating structures makes systems integration (for e.g., for enabling effective liquidity management) challenging.

Suboptimal Testing approaches

- Lack of standard enterprise-wide compliance testing approaches. There is an overreliance on manual testing methods.
- Operational and compliance risks testing are executed in silos. Also, compliance testing within the individual LOBs is done in a silo. This leads to inconsistent application of compliance procedures and policies across LOBs.
- While strong forensic testing capabilities exist in banks for AML / BSA transaction monitoring, fair lending, and call monitoring, it is leveraged on ad-hoc basis in most other business areas.

Data

About the Author

Anjani Kumar

Principal Consultant, Consumer and Commercial Banking group, FS, Infosys

Anjani has over 18 years of comprehensive IT, domain and process consulting experience. Currently, he manages several strategic initiatives including the Competency Development Program and thought leadership showcasing efforts. Over the years, he has provided consulting services and managed many large and critical IT engagements for numerous clients. He was also recognized as the lead process auditor for the banking division of a major global bank. He has extensive techno-functional skills in the banking domain, especially in the channels, analytics, and core banking space, and an in-depth understanding of quality and process models – CMMI, Six Sigma, ITIL, etc. Anjani holds a Bachelor of Engineering degree from IIT Roorkee and, over the years, has earned many reputed and industry-recognized domain and process certifications.

He can be reached at anjani_kumar@infosys.com

For more information, contact askus@infosys.com

Infosys be more