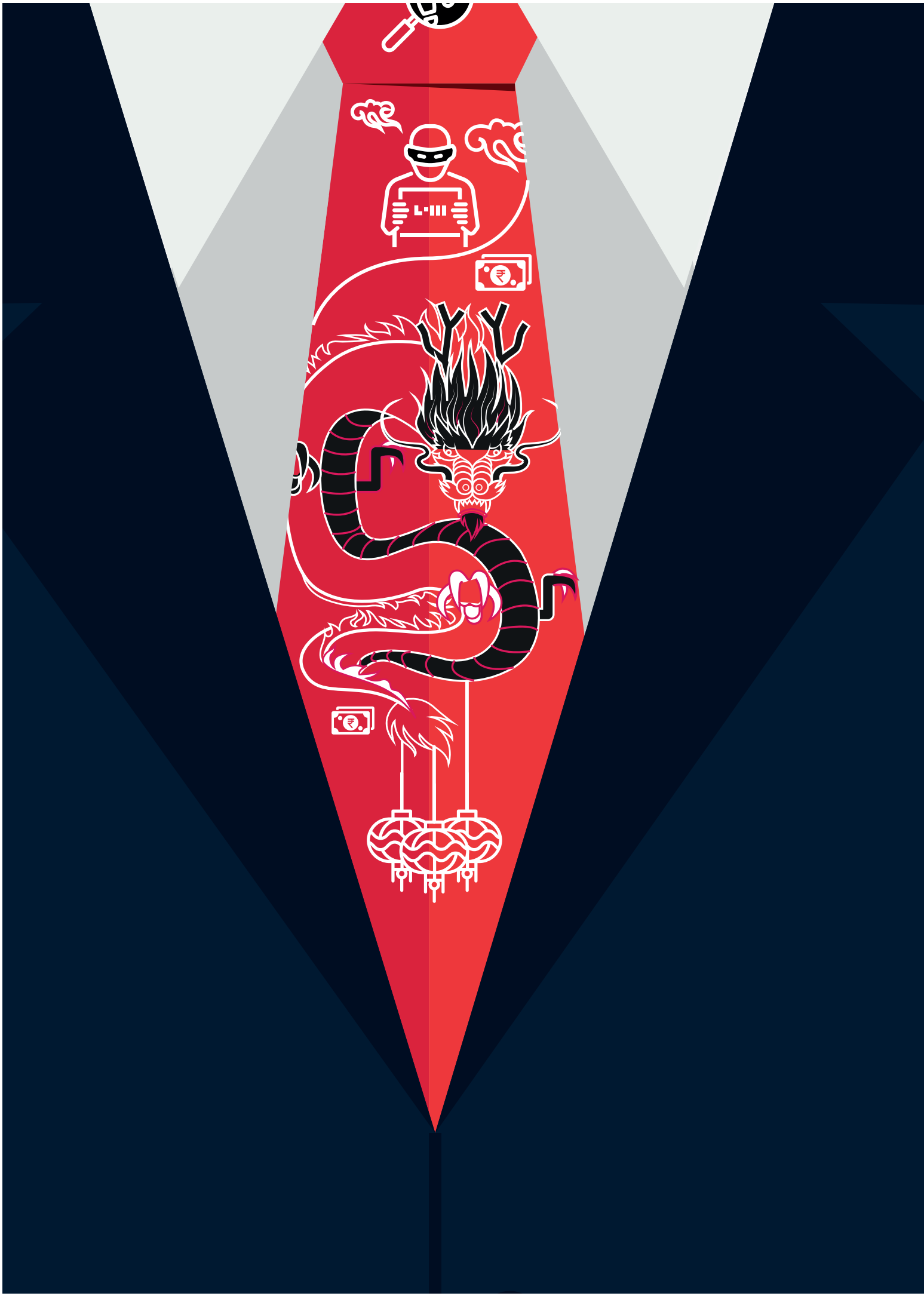

GETTING A HANDLE ON FINANCIAL CRIME COMPLIANCE IN SOUTHEAST ASIA

Regulatory compliance, the beasts of burden? With the avalanche of shifting regulatory requirements and new criminal threats, the investment management sector will have to innovate and evolve compliance frameworks as well as rethink current day models.

Radish Singh
Partner
Forensic
Deloitte

Managing financial crime compliance is becoming increasingly critical for investment management (IM) firms such as investment asset managers, retail fund providers, edge funds, wealth managers, investment platforms, and asset service providers in Southeast Asia (SEA).

Financial crime threats in SEA

Financial institutions in Singapore and Malaysia—two strategic locations with porous borders and open economies—face the threat of money laundering. IM firms in these two countries are particularly at risk of being conduits for money laundering with their primary business of receiving and making investments internationally susceptible to such crime.

In light of this, the regulators in Singapore and Malaysia have developed specific Anti-Money Laundering (AML) and Counter Terrorist Financing (CFT) regulations to impose compliance requirements on IM firms in order to manage the AML/CFT risks to which they are exposed. These regulators have set a strict tone on the tightening of governance, Customer Due Diligence (CDD) processes, and strengthening of internal controls.

With these constant updates, the regulatory bar is rapidly rising. Keeping this in mind, what do IM firms have to look out for and how can they develop their Financial Crime Compliance (FCC) framework to meet the ever-changing regulatory requirements and expectations?

First, we must consider the common regulatory themes when developing an FCC framework. Malaysia revised its Guidelines on Prevention of Money Laundering and Terrorism Financing for Capital Market Intermediaries in 2014 and Singapore published its amended Prevention of Money Laundering and Countering the Financing of Terrorism – Capital Markets Intermediaries in 2015. While regulations in these two countries differ, IM firms in both Malaysia and Singapore should take note of four key regulatory themes:

a) **Applying a risk-based approach**
   IM firms are required to develop sound policies and procedures to manage risk. Based on these policies and procedures, these institutions need to perform a risk assessment, monitoring risk mitigation of money laundering and terrorism financing risks.

b) **Screening new launches for money laundering and terrorism financing risk**
   New products and technologies need to be screened for money laundering and terrorism financing risk, and necessary approval is required before products, practices, and technologies can be launched.

c) **CDD for all customers**
   Screening is mandatory for all customers, natural persons appointed to act, connected parties, and beneficial owners, regardless of risk profiles. All IM firms are expected to perform ongoing monitoring of their customers and detect money laundering and terrorism financing risks. In addition, firms must identify the beneficial owner of entities and trusts that they are working with. Regulators in both countries allow the use of the threshold of 25 percent ownership to identify the natural person who ultimately owns the legal person or arrangement.

d) **Reliance on third parties and group policy**
   The guidance in both Singapore and Malaysia allows for the use of third parties by firms when performing CDD, but sets out limitations in terms of the extent to which these third parties can be used. For example, in Malaysia, IM firms must apply a risk lens to discern the reliance on third parties they engage; where the key consideration is the extent the third party has applied recommendations from the Financial Action Task Force on Money Laundering (FATF). Firms are prohibited from relying on third parties to verify the beneficial owner and those located in higher risk jurisdictions. In Singapore, there is a requirement for IM firms to implement group policies and procedures for its branches and subsidiaries within the financial group to share information required for the purposes of CDD, and for money laundering and terrorism financing risk management. Furthermore, the Singapore regulations do not allow third parties to perform ongoing monitoring for the IM firm. Reliance on third parties is subject to appropriate assessment and proper arrangement with the third party that the IM firm is relying upon.

Malaysia revised its Guidelines on Prevention of Money Laundering and Terrorism Financing for Capital Market Intermediaries in 2014 and Singapore published its amended Prevention of Money Laundering and Countering the Financing of Terrorism (Capital Market Intermediaries) in 2015.

"Effectiveness" is the new buzzword
In the current landscape, compliance will only get more challenging and costly. So what can firms continue to do to enhance their financial crime compliance framework?

Getting the correct FCC compliance target operating model sounds simple. However, the more complex the IM firm and its business, the more challenging it is to administer control and surveillance. In addition to the business-as-usual activities, ensuring effective responses to address tightening regulatory changes and increasing regulatory expectations demands equal attention.

It is important for the compliance culture to shift from being process-driven to being "risk aware" in order to appreciate the complexities of the FCC operating models, and appropriately adapt in response to new threats and emerging typologies with its associated red flags.

While it may be tall order, a good starting point is to develop three lines of defense—the front office, compliance, and audit—with calibrated risk tolerance principles that work like a well-oiled engine to detect and prevent financial crime. This demonstrates, inter alia, that the IM firm has a good grip on its "single client view" and is effective in monitoring and managing FCC risk.

Board governance and management supervision must be demonstrable. Although easier said than done, there is a need for evidence-clear reporting, the provision of good-quality risk dashboards, and clear channels to escalate key findings. The boards and management should be actively involved in critical decisions in the management of FCC risk for the organization.

The FCC risk assessment across the IM firm and lines of business needs to be effective in calculating inherent risk and assessing the robustness of controls to manage such risk. The outcome of the risk assessment must—and it is critical that it does—inform the overall framework, policies, procedures, process architecture, people, technology, customer risk profiling, monitoring, and assurance exercise as well as help design the Money Laundering Reporting Officer (MLRO)'s dashboard to the management.

It is important for the compliance culture to shift from being process-driven to being "risk aware" in order to appreciate the complexities of the FCC operating models, and appropriately adapt in response to new threats and emerging typologies with its associated red flags.

While the subject may not sound exciting, it is worth repeating the importance of continuously beefing up the gatekeeping function, i.e., performing robust Know Your Customer (KYC)/CDD processes. The better the quality of the CDD process, the better the ability of the IM firm to assess customer risk and monitor the relationship on an ongoing basis. Firms need robust regimes to not only identify risks at the point of onboarding but monitor such risks throughout the lifecycle of the customer with the firm.

To do so, IM firms will need to separate their operational and advisory functions. It is important that the employees who have "business-as-usual" tasks and those that ensure the effectiveness of the controls framework are not one and the same.

IM firms should also be aware of the evolution in trade finance compliance or trade-based money laundering compliance and correspondent banking relationships oversight. For their trade business, firms need to institutionalize a framework that broadly addresses the review of risk through the trade documentation, trade routes and vessels, screening of parties, assessment of the legitimacy of goods (from dual use risk and under/overpricing), and whether sanctioned parties or countries are involved. There is very little appetite from regulators for failures in the compliance framework for IM firms that undertake trade finance business or establish correspondent banking relationships.

In addition, having a transaction monitoring system that focuses on link analysis can help. This allows for common sources of wealth or ultimate beneficial owners'

transactions to be assessed holistically. IM firms should make more investments in analytics to optimize the transaction monitoring technology to improve the effectiveness of the monitoring as well as the challenge and audit abilities.

IM firms should also look into the documentation of the overall control architecture, which includes the labyrinth of processes and technologies put in place to mitigate FCC risks. This can be documented as a single source of truth and assessed to ascertain whether the controls environment meets regulatory standards and whether there is more work needed to plug gaps.

Continued vigilance

The FCC framework will continue to evolve in line with the changing business landscape and regulations are expected to tighten.

When implementing a risk-based approach, identifying key indicators where the IM firm needs to perform a deep-dive analysis to address any potential risks, and the sufficiency of controls in place to manage such risk, is essential. The regulatory bar on financial institutions (FI), including IM firms, in Singapore and Malaysia have risen so much today that "risk-based approach" translates to "heightened risk-based approach" when designing AML/CFT frameworks and assessing associated risks and controls. Compliance frameworks simply need to be prudent and defensible in today's regulatory environment.

In addition, with the recent actions instituted by regulators in both Malaysia and Singapore on certain FIs, the regulatory arbitrage should narrow fairly swiftly with industry participants expected to further tighten compliance efforts. IM firms in SEA will also be required to invest more in this area as they harmonize their global regulatory standards and guidelines across their footprint markets. The natural consequence of this will arguably be increased compliance costs with resultant thinning profit margins for some.

However, it is important for FCC leaders to keep in mind that the monetary penalties for non-compliance and damage to a firm's reputation far outweigh the cost of compliance. On the plus side, this may call for integration or more innovation in business, cost effective service delivery models, digitization and compliance efficacy, and use of utilities that can operate within the regulatory regime without impediments to not just reduce cost, but also manage risks.

While the subject may not sound exciting, it is worth repeating the importance of continuously beefing up the gatekeeping function, i.e., performing robust Know Your Customer (KYC)/CDD processes. The better the quality of the CDD process, the better the ability of the IM firm to assess customer risk and monitor the relationship on an ongoing basis.

To the point:

- Managing financial crime compliance is becoming increasingly critical for IM firms.
- Regulators in Singapore and Malaysia have developed specific regulations to impose compliance requirements on IM firms to manage AML/CFT risks to which they are exposed and have set a strict tone on the tightening of governance, CDD processes, and strengthening of internal controls.
- It is important for the compliance culture to shift from being process-driven to being "risk aware" in order to appreciate the complexities of the FCC operating models.
- A good starting point is to develop three lines of defense—the front office, compliance, and audit—with well-calibrated risk tolerance principles to detect and prevent financial crime.
- Board governance and management supervision must be demonstrable.
- FCC risk assessment across the IM firm and lines of business needs to be effective in calculating inherent risk and assessing the robustness of controls to manage such risks.
- The better the quality of the CDD process, the better the ability of the IM firm to assess customer risk and monitor the relationship on an ongoing basis.
- The regulatory bar on FIs in SEA has risen so much today that a "risk-based approach" translates to a "heightened risk-based approach".