Report on the Weaknesses of the Corporate Governance Guidelines for Banks and Other Financial Institutions (April 2015) in the Context of Seychelles.

By Fadeke Ayoola

The Corporate Governance Guidelines for Banks and Other Financial Institutions in Seychelles that came into effect in April 2015 provide a critical framework for effective governance. However, in Seychelles—given its unique financial and economic characteristics—certain weaknesses are particularly pronounced. For example, financial institutions are generally smaller in scale and may lack the resources required to implement the robust recommendations laid out in the guidelines. Limited access to expertise, financial support, and human resources can create difficulties in fully adhering to governance standards, leading to gaps in compliance and oversight.

The principle of proportionality is intended to accommodate variations in the size and complexity of institutions. However, the lack of clear benchmarks or criteria for its application may result in inconsistent interpretations among institutions in Seychelles. Without standardized guidance, proportionality could inadvertently weaken governance standards.

While Seychelles has a relatively small financial sector, it is not immune to emerging global risks, including cybersecurity threats, environmental vulnerabilities, and disruptions from technological advancements. The 2015 guidelines provide insufficient direction on addressing these evolving challenges, leaving institutions inadequately prepared to mitigate their impact. For example, cybersecurity poses a significant and continually evolving risk for financial institutions. The absence of specific guidance in the 2015 guidelines leaves institutions vulnerable to breaches, data theft, and financial losses.

An effective cybersecurity strategy hinges on the interplay of preventive, detective, and corrective controls, along with robust governance. Preventive measures, such as access controls, firewalls, encryption, and intrusion prevention systems, act as the first line of defence, protecting sensitive data and systems from unauthorized access and attacks. However, no preventive measure is foolproof, making detective controls essential. By employing real-time alerts and intrusion detection systems, organizations can promptly identify suspicious activities, reducing potential exposure. Should a breach occur, corrective controls come into play, including well-defined incident response plans and recovery mechanisms to minimize operational and reputational damage. Governance ties all these efforts together, with boards embedding cybersecurity into the organization's overall risk management

framework. This ensures continuous oversight, resource allocation, and alignment with strategic priorities, creating a comprehensive and adaptive defence against cyber threats.

Seychelles faces unique environmental risks, including rising sea levels and climate-related disasters. These factors can disrupt business continuity, impact financial stability, and pose reputational risks for financial institutions. Effective internal controls for managing environmental risks must encompass risk assessments, business continuity planning, and reporting mechanisms. Organizations should integrate environmental risk assessments into their control frameworks to evaluate potential impacts on operations, assets, and long-term sustainability. Alongside this, robust business continuity plans are crucial for maintaining operational resilience during environmental disruptions, ensuring that core functions can adapt to and recover from crises effectively. Additionally, consistent and transparent reporting mechanisms should be established to monitor and communicate environmental risks, aligning with global Environmental, Social, and Governance (ESG) standards. This integrated approach not only enhances organizational preparedness but also strengthens stakeholder confidence by demonstrating a proactive commitment to environmental stewardship.

The rise of fintech, digital transformation, and automation offers significant opportunities for efficiency and innovation but also introduces risks, such as outdated systems and a growing need for skilled personnel. From an internal control perspective, it is essential to implement continuous technology upgrades, ensuring that systems remain compatible with emerging technologies and are resilient against obsolescence. Equally important is investing in comprehensive training and development programs to equip employees with the knowledge and skills required to operate and secure modern systems effectively. Furthermore, robust vendor management controls must be established to assess and monitor third-party providers, particularly those handling critical technological functions, to mitigate risks associated with outsourcing and external dependencies. Together, these measures help organizations harness the potential of new technologies while safeguarding their operational integrity.

Addressing emerging risks necessitates an integrated internal control approach that includes proactive governance, dynamic risk assessments, regulatory collaboration, and robust audit functions. Boards and management must prioritize emerging risks within their governance agenda, ensuring internal controls are aligned with these evolving challenges. Risk assessments should be updated regularly to account for new trends and threats, keeping organizations responsive to the changing environment. Collaboration with regulators is essential for developing localized frameworks that address specific risks faced by institutions in Seychelles. Additionally, independent audits play a crucial role in evaluating the effectiveness of existing controls and providing actionable recommendations for continuous improvement. This comprehensive approach ensures that institutions remain resilient in the face of emerging risks.

Addressing emerging risks through internal controls is not merely a compliance activity; it is a strategic necessity to safeguard Seychelles' financial sector. By embedding risk-specific controls and fostering a culture of adaptability, financial institutions can better prepare for and mitigate the impacts of global challenges. The guidelines emphasize board competence but do not adequately enforce board independence. In Seychelles, where financial institutions may be closely held or family-owned, this oversight increases the risk of conflicts of interest, reducing the effectiveness of governance mechanisms.

To strengthen governance in Seychelles, several key recommendations should be considered. First, capacity-building initiatives are essential, such as tailored training programs for board members and access to shared governance resources, while partnerships with regional and international organizations can provide necessary technical assistance. Second, the proportionality principle requires clear, localized guidelines that align with Seychelles' financial environment and regulatory capacity, including illustrative examples to support consistent application. Third, the guidelines should be updated to address emerging risks, such as climate-related vulnerabilities, cybersecurity threats, and fintech developments, while fostering collaboration among institutions to create stronger collective responses. Lastly, board independence must be enhanced by mandating a higher proportion of independent directors and providing detailed guidance on their qualifications and roles, ensuring greater transparency and effective oversight across financial institutions. This integrated approach will reinforce governance practices and resilience within Seychelles' financial sector.

Conclusion

While the 2015 Corporate Governance Guidelines provide a valuable foundation, their relevance and effectiveness in Seychelles require adjustments to address the unique challenges faced by the country's financial sector. Incorporating these recommendations will not only strengthen governance practices but also enhance the resilience and sustainability of financial institutions in Seychelles.