



Central Bank of Sri Lanka

NEWS SURVEY

Volume 44 Number 4 October - December 2024

IN THIS ISSUE

- 02 *Playing by the Rules: Numerical Fiscal Rules for Fiscal Sustainability*
- 10 *Pivotal Role of the Chief Information Security Officer (CISO) in Financial Sector*
- 21 *Collaboration and Knowledge Sharing in Cyber Security*
- 26 *Strengthening Legal Framework applicable for Licensed Banks: Amendments to the Banking Act*
- 32 *Central Bank Communication for Effective Monetary Policy Implementation*



0 009042 499841

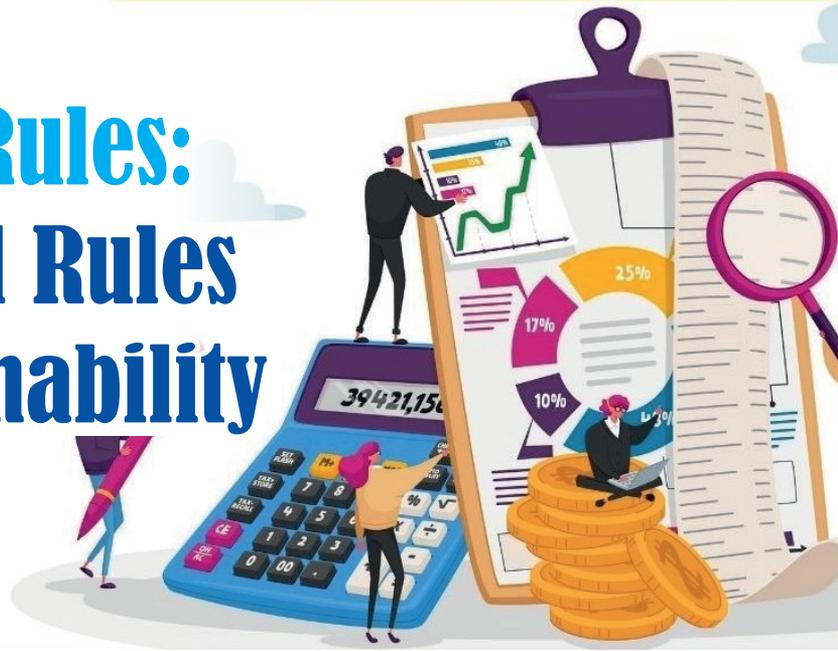
ISSN 1391 3589

The views expressed in the articles are those of the writers and are not necessarily those of the Central Bank of Sri Lanka.

Price per copy: Rs. 80.00
Annual subscription (Inclusive of postage): Rs. 500.00

Playing by the Rules: Numerical Fiscal Rules for Fiscal Sustainability

Dr. S P Y W Senadheera
Deputy Director
Economic Research Department



1. What are Fiscal Rules?

Fiscal rules are long term constraints imposed on fiscal policy by placing numerical limits on fiscal aggregates, such as expenditure, debt and revenue (Budina, et al., 2013).¹ These rules aim at fostering fiscal discipline, ensuring debt sustainability and building credibility on public financial management (Kopits & Symansky, 1998). During the past three decades, fiscal rules have become a widely used policy tool for restraining fiscal profligacy, with advanced countries being the forerunners of adoption of these rules. Fiscal Rules Dataset (1985-2021) of the International Monetary Fund (IMF) shows that only a handful of countries were following fiscal rules until early 1990s, but since then, the adoption of fiscal rules gained traction with many emerging and developing countries following the lead of advanced economies. While

¹ Fiscal rules can be in the form of numerical rules on fiscal aggregates or procedural rules on the budgetary process. These procedural rules are expected to establish good governance and practices, ensure transparency and improve predictability. In many countries, both numerical and procedural rules are being implemented in tandem. However, this article focuses only on numerical fiscal rules.

the rise in number of countries following fiscal rules in 1990s was driven by the European Union members, the surge in public debt during global financial crisis (GFC) accelerated the fiscal rule adoption across the world in the wake of the GFC. Accordingly, 105 countries were following fiscal rules by 2021.

In theory, the policymakers should follow countercyclical fiscal policies by running budget deficits during economic downturns and reverting to budget surpluses during economic booms. However, in practice, governments tend to run budget deficits both during recession times as well as in the upswings in the business cycle and financing these deficits through borrowings. Since policymakers often have incentives to pursue policies that would raise expenditure to benefit their own constituency, governments generally fail to generate budget surpluses during economic booms to pay off the debts that were amassed during recessions. This leads to accumulation of government debt posing challenges to debt sustainability. Short-run political expediency that result in ‘deficit biasness’ provides the rationale for introducing institutional mechanisms to constraint

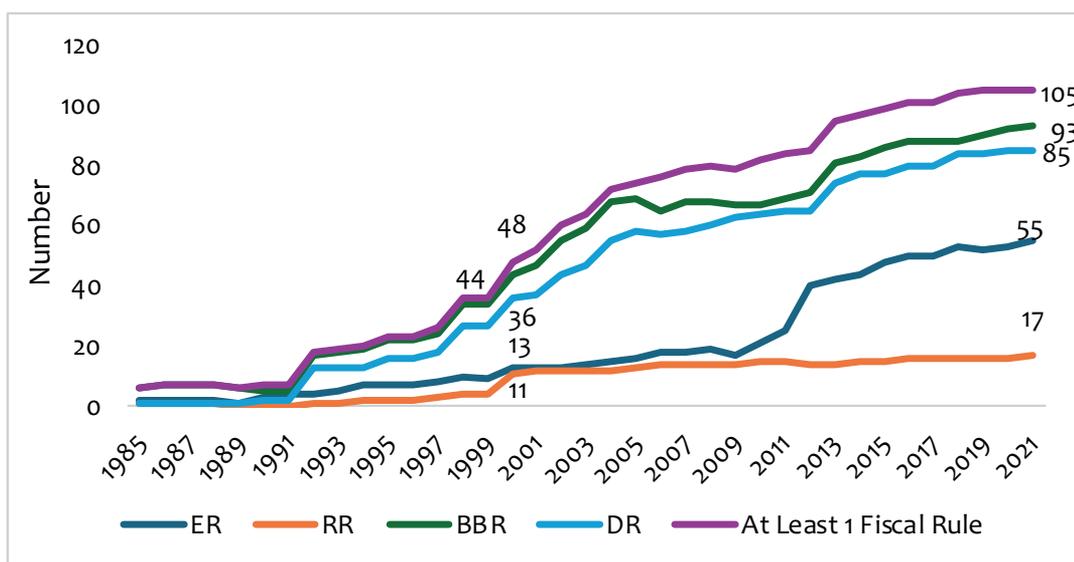
the governments’ discretion over fiscal policy. Numerical fiscal rules are one such institutional mechanism, where policymakers’ discretion in manoeuvring fiscal policy is restrained by the numerical limits imposed on fiscal aggregates.

2. Types of Fiscal Rules

Based on the fiscal aggregates constrained by the rule, four categories of numerical fiscal rules can be identified, namely, debt rules, budget balance rules, expenditure rules and revenue rules. Many countries use a combination of fiscal rules since individual fiscal rules are not equally apt in achieving different macroeconomic objectives

(a) Budget balance rules: Budget balance rules are numerical limits imposed on different types of budget balances, such as the overall budget balance, cyclically adjusted balance,² structural/underlying fiscal balance³, the ‘average fiscal balance over the business cycle’ or the primary balance. Since most components of the budget balance are under the control of the policymakers, many budget balance rules can be used to ensure debt sustainability while providing operational guidance for policymakers to control the evolution of debt ratio. Despite interest expenditure being beyond the control of the policymakers, adhering only

Figure 1: Number of Countries Adopting Fiscal Rules



Note : ER= Expenditure Rules, RR=Revenue Rules, BBR= Budget Balance Rules, DR=Debt Rules

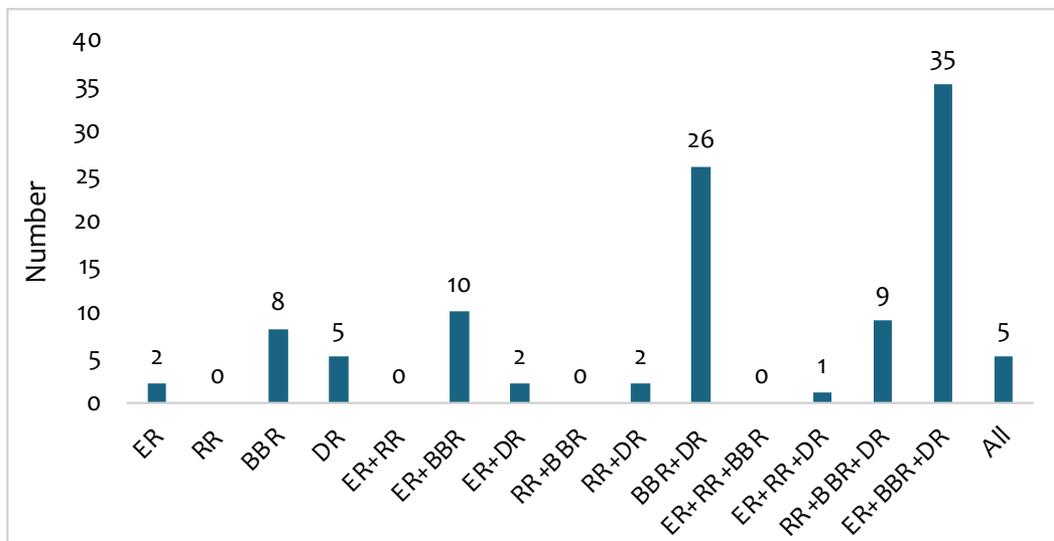
Source: Fiscal Rules Dataset 1985-2021, IMF

such as economic stability, debt sustainability and limiting the size of the government. For example, a debt rule combined with an expenditure or structural budget balance rules could be more appropriate for addressing debt sustainability issues. The number of countries following fiscal rules and different combinations of fiscal rules are given in Figure 1 and Figure 2 below.

to a primary balance target may weaken the effectiveness of achieving debt sustainability

- The budget balance that would have been recorded if the economy was operating at full potential (i.e., when the GDP is equal to the potential GDP) is called cyclically adjusted balance.
- The structural/underlying fiscal balance is estimated by deducting expenditure from revenue, after adjusting both revenue and expenditure for the effects that are attributable to one-off events and the economic cycle.

Figure 2: Number of Countries Adopting Different Combinations of Fiscal Rules – 2021



Note : ER= Expenditure Rules, RR=Revenue Rules, BBR= Budget Balance Rules, DR=Debt Rules

Source: Fiscal Rules Dataset 1985-2021, IMF

targets since large interest expenditure could also result in debt accumulation.

Although the overall budget balance rule is widely understood and easily communicated, it lacks economic stabilisation features and hence may not be helpful in reducing the debt to Gross Domestic Product (GDP) ratio. On the other hand, cyclically adjusted balance, structural balance and ‘average fiscal balance over the business cycle’ rules explicitly account for the business cycle effects. However, estimating this business cycle effect, particularly by estimating the output gap, is a challenging task and hence, these rules cannot be easily communicated or monitored. In addition, under ‘average fiscal balance over the business cycle’ rule, policymakers may opt to postpone the implementation of required policy adjustments towards the end of the business cycle resulting in sub-optimal outcomes (Budina, et al., 2013). 93 countries including Indonesia, Israel, Australia, New Zealand, Japan, United Kingdom (UK), India and Pakistan have been using budget balance rules by end 2021.

(b) Debt rules: Under these rules, an explicit numerical limit or a target will be imposed on the government/ public debt, expressed as a percentage of GDP. Debt rules are generally easily understood and communicated to the stakeholders. They are effective in ensuring the convergence of debt to a sustainable level. However, debt could be affected by exogenous factors that are beyond the control of the government, such as movements in the interest rates and exchange rates, warranting unrealistic policy adjustments to adhere to the fiscal rule. Further, fiscal policy adjustments affect the debt levels with a time lag and hence, debt rules would not provide a distinct and binding short-term guidance for the policymakers, especially when the debt levels are well below the ceiling. On the other hand, when the debt levels are near the debt ceiling and the rule becomes binding, debt rules could result in procyclical fiscal policy, especially when the economy is hit by an economic shock (Budina, et al., 2013). By end 2021, debt rules were in place in 85 countries

including India, Netherlands, Portugal, United Kingdom, Vietnam and Indonesia.

(c) Expenditure Rules: These rules impose numerical limits on the total, primary or current expenditure of the government either in absolute terms or on the growth rates or seldomly, as a percentage of GDP. Expenditure ceilings are less complicated to understand, easily monitored and can be used to control the size of the government through constraints on spending. Unlike budget balance rules and debt rules, expenditure rules are not directly linked with the debt sustainability objective as they do not impose any limit on revenue. Expenditure rules do not necessarily address the bias toward large deficits, especially ones that stem from large tax cuts or systematic overoptimistic revenue projections (Sanchez, et al., 2003). However, expenditure rules, when used in combination of debt or budget balance rules, could be a valuable tool for prompting fiscal consolidation to be in line with the debt sustainability targets.

Moreover, expenditure rules allow countercyclical fiscal policy, thereby contributing to economic stability. During periods of temporary revenue excesses, especially with windfall revenue receipts, expenditure rules would limit fiscal extravagance. In contrast, countercyclical fiscal policies would not be constrained by expenditure rules during economic shocks despite low revenue collection. The countercyclical nature of the expenditure rules would be more profound if the rule is designed by excluding expenditure that are sensitive to the business cycle, such as unemployment benefits (Budina, et al., 2013). However, this countercyclicality of the expenditure rules will

be at the expense of debt stabilisation objective. 55 countries such as the United States of America (USA), Australia, France, Finland, Netherlands, Portugal, Russia, Singapore and Thailand have been following expenditure rules by end 2021.

(d) Revenue Rules: These rules can be imposed as floors (or ceilings) for government revenue with the objective of improving revenue collection (or reducing taxpayers' burden), or by determining the use of windfall revenue. Generally, except for the limits placed on the utilisation of windfall revenue, establishing revenue targets is challenging due to the procyclicality of revenue collection. Further, revenue rules are not effective in terms of debt stabilisation as they do not constraint government spending. Moreover, revenue ceilings or floors, when used in isolation, cannot deter procyclicality of fiscal policy as these rules do not account for the effect of automatic stabilizers over the business cycle. Nevertheless, similar to expenditure rules, revenue rules can be used to limit the government size, especially when limits are set on the utilisation of windfall revenue (Budina, et al., 2013). Revenue rules are less popular and are used only by 17 countries by the end of 2021. Australia, France, Iran, Kenya, Netherlands and Vietnam are some of the countries who follow revenue rules.

3. Effectiveness of Fiscal Rules in Improving Fiscal Sustainability

Adhering to fiscal rules brings numerous benefits to an economy, though appropriate design and flexibility in the rules result in better macroeconomic outcomes. Ardanaz, et al. (2021) show that stronger fiscal performance, i.e., higher primary balance, is associated with the presence of expenditure rules.

Meanwhile, Badinger and Reuter (2017) reveal that countries with more stringent fiscal rules tend to have higher fiscal balances (i.e., smaller deficits), low output volatility and lower interest rate spread on government securities. Sawadogo (2020) finds that fiscal rules widen the market access of developing countries by narrowing sovereign bond spreads and increasing the sovereign debt ratings of such economies. Nevertheless, Ardanaz, et al. (2023) point out that fiscal rules are not a panacea for enhancing fiscal performance. They argue that the quality of the rule design, mechanism for ensuring compliance, forward guidance on return to rule in the event of a deviation and effects on the spending composition could determine the effectiveness of fiscal rules on improving fiscal performance, the countercyclicality of fiscal policy and debt sustainability. Several key features that augment the effectiveness of rule-based fiscal policy frameworks are discussed below.

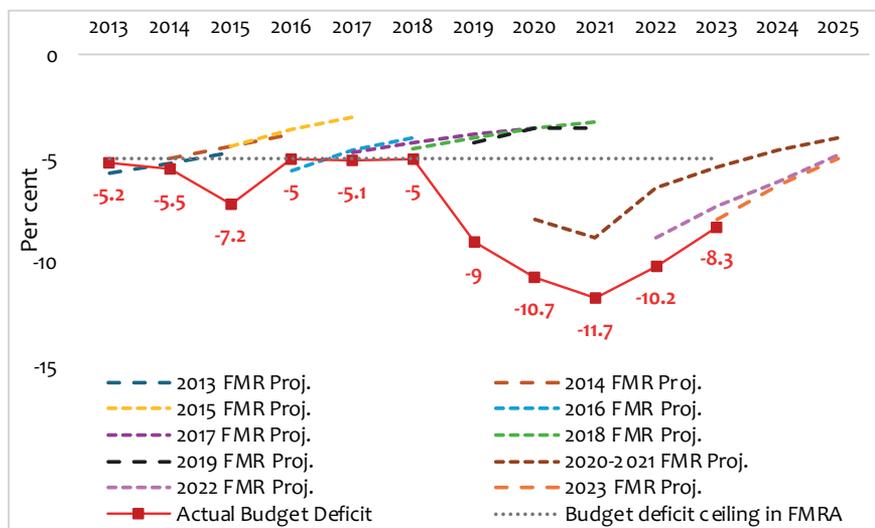
- ***Flexibility of the rules to accommodate economic shocks:*** Stringent fiscal rules could deter the governments in responding to economic shocks with countercyclical policies. Well-defined escape clauses allow the countries to temporarily exceed the limits imposed by the fiscal rules during exceptional circumstances such as natural disasters, economic downturns or situations that threaten national and public health security, without breaching, suspending or abandoning the rule permanently. Such clauses establish a clear plan on how the governments should proceed in the event of an unanticipated severe crisis and how to revert to compliance in the aftermath of the shock. Hence, escape clauses enhance the fiscal credibility during crisis periods. During COVID-19 pandemic, many countries invoked the escape clauses embedded in their fiscal rules, creating space for the governments to increase

their spending on combating the public health hazard and supporting businesses and households affected by the economic downturn.

- ***Legal Basis of Fiscal Rules:*** While fiscal rules can be stated as a government commitment, the durability and credibility of the rule can be ensured by strengthening the legal basis of the rule by integrating it in budget laws, constitution or in international treaties (in the case of supranational fiscal rules).
- ***Monitoring and Enforcement:*** Many countries adopt formal enforcement measures in relation to fiscal rules especially by integrating the rules in the medium-term fiscal framework and the budget preparation process. In many instances, independent institutions such as fiscal councils⁴ are established to verify the ex-ante and ex-post compliance of the government with the fiscal rules. While many countries have correction mechanisms that stipulate the actions to return to the fiscal rule in the event of deviation (e.g., many European Union countries, Panama and Peru), some may opt for pre-emptive actions that are triggered as the country reaches the limits set out by the fiscal rules. For example, Poland has such pre-emptive actions of varying degree of fiscal adjustments that are activated as the debt level approaches the debt ceiling (Davoodi, et al., 2022). Meanwhile, sanctions or fines can also be imposed to discourage non-compliance with fiscal rules (e.g., in European Union).

⁴ Fiscal councils are independent public entities holding a statutory or executive mandate to foster sustainable public finance management by assessing fiscal plans and performance, monitoring compliance with fiscal rules, ascertaining macroeconomic and budgetary forecasts, and costing new fiscal policy measures (International Monetary Fund, 2013). A fiscal council would promote fiscal stability and transparency, thereby increasing the reputational and electoral cost of undesirable policy actions and renewed commitments of the governments (Davoodi, et al., 2022).

Figure 3: Budget Deficit Forecasts and Realised Budget Deficits



Sources : Ministry of Finance
Central Bank of Sri Lanka

4. Fiscal Rules in Sri Lanka

Several fiscal rules were in place in Sri Lanka since 2003, under the Fiscal Management Responsibility Act, No. 3 of 2003 (FMRA). Accordingly, limits had been imposed on the overall budget deficit and government guaranteed debt while a government debt target was to be achieved within specific periods. However, these rules have not been effective in containing fiscal profligacy over the years. In many instances, the limit on budget deficit of 5 per cent of GDP was ignored by successive governments during the budget preparation and approval process as well as in annual fiscal performance reviews. The budget deficit forecasts published in the Fiscal Management Reports (FMR) of the Ministry of Finance and the realised budget deficits are depicted in Figure 3. Lack of formal enforcement mechanisms or strong accountability requirements under the FMRA allowed policymakers to disregard the budget balance rule without any immediate repercussion. Meanwhile, the limit on government guaranteed debt was revised upward several times through legislative amendments when the limit became binding. In terms of government debt, the

debt target and deadline to achieve the target were also revised a few times once a specific milestone was reached without bringing down the debt level to the targeted level. Despite the fiscal rules that were imposed through legislation, non-adherence to fiscal rules and lack of accountability for non-compliance resulted in perpetual budget deficits, which were well above the budget estimates, leading to debt accumulation up to an unsustainable level by 2022.

In response to the unsustainable debt level and ensuing economic crisis in 2022, the Government embarked on a reform programme of fiscal consolidation and economic stabilisation under the Extended Fund Facility of the International Monetary Fund (IMF-EFF) in tandem to the restructuring of debt portfolio of the Government. While the IMF-EFF supported programme and debt restructuring are expected to ensure fiscal and debt consolidation during the programme period, sustaining fiscal discipline in the long term is also paramount. Accordingly, under the IMF-EFF programme, a new piece of legislation, the Public Financial Management Act, No. 44 of 2024 (PFM

Act) was enacted in August 2024 with the aim of ensuring fiscal prudence while strengthening accountability, transparency and governance of public financial management of the country. This PFM Act has introduced a couple of fiscal rules in terms of a ceiling on primary expenditure and a ceiling on government guaranteed debt.⁵

The primary expenditure rule intends to restrain fiscal profligacy, which is key for the ongoing fiscal consolidation efforts. However, expenditure rules can act as a barrier for long-term economic growth as policymakers tend to cutdown capital expenditure amidst rigid recurrent expenditure in instances where the rule is binding. In emerging market economies, expenditure rules are generally associated with lower levels of public investment in the absence of effective public financial management systems to prevent policymakers from postponing high-quality discretionary spending for the sake of complying with the rule (Cordes, et al., 2017). Nevertheless, Ardanaz, et al. (2021) posit that flexible fiscal rules which consist of mechanisms to accommodate exogenous shocks,

5 Although PFM Act does not specify numerical fiscal rules for primary balance or the public debt, the recently enacted the Economic Transformation Act, No.45 of 2024 (ETA) also sets out five fiscal rules. Accordingly, ETA stipulates fiscal rules in relation to public debt (95 per cent of GDP by 2032 and thereafter), primary balance (2.3 per cent of GDP till 2032 and at least 2 per cent of GDP thereafter), government revenue (at least 15 per cent of GDP from 2027 onwards), gross financing needs (below 13 per cent of GDP by 2030 and thereafter) and foreign debt service payments (4.5 per cent of GDP by 2027 and thereafter). These rules provide a legislative backing for the targets that have been laid by the current economic reform programme under the IMF-EFF. Nevertheless, enforcement mechanism and accountability requirements related to these fiscal rules are not enshrined in said legislation, and the enforcement of these rules would be assured only through the continuation of the IMF-EFF supported programme. Therefore, strong political commitment to adhere to these fiscal rules is paramount to achieve the intended fiscal objectives.

such as well-defined escape clauses, cyclically adjusted fiscal targets and differential treatment on government investment expenditure, have a minimal impact on public investments, though stringent fiscal rules can have a negative effect on spending on investments. The primary expenditure rule in the PFM Act consists of an escape clause allowing to deviate from the rule under exceptional circumstances that are specified in the PFM Act, namely natural disasters, or threats to national security or public health and safety which require additional spending beyond the budget. The Minister is required to obtain Parliamentary approval for these deviations.

Although the primary expenditure ceiling under the PFM Act, which is set at 13 per cent of nominal GDP,⁶ seems reasonable at present given the low revenue mobilisation in the country, this level is far below compared to the spending levels of peer economies. During 2015-2023 period, the average primary expenditure in middle income and emerging economies was circa 30 per cent of GDP. In the event that Sri Lanka is able to persistently achieve a higher revenue mobilisation well over 15 per cent of GDP,⁷ the Government could consider raising the primary expenditure ceiling in the future through a legislative amendment, allowing the economy to be benefitted from higher revenue collection without jeopardising the debt reduction objective of the Government.

The ceiling on government guarantees⁸ under the PFM Act aims for debt sustainability by limiting the risk of realisation of contingent liabilities. The PFM

6 The primary expenditure ceiling will be expressed in nominal terms calculated based on the nominal GDP estimate of the Ministry of Finance.

7 Revenue floor under the Economic Transformation Act

8 The aggregate stock of outstanding government guarantees at the end of each financial year shall not exceed 7.5 per cent of the average GDP of the relevant financial year and preceding two financial years. This limit will be reviewed every five years to ensure it is in line with the debt reduction objective of the government.

Act stipulates procedural rules related to primary balance and debt by requiring the preparation of fiscal strategy statement and the annual budget in accordance with the debt reduction objective of the Government.

5. Conclusion and Way Forward for Sri Lanka

Many developed and developing countries have embraced fiscal rules to maintain government finances on a sustainable trajectory. However, the adoption of fiscal rules per se will not guarantee the effectiveness of the rules, but the appropriate mix and design of the rules, legislative support as well as adequate monitoring and enforcement mechanisms would be key to achieve anticipated fiscal objectives. This was evident through the Sri Lankan experience, as fiscal rules under the FMRA failed to yield desired outcomes owing to weak enforcement mechanism and lack of accountability for non-compliance. Discretionary fiscal policies of successive populist governments in Sri Lanka resulted in several decades of fiscal profligacy that culminated in a debt crisis in 2022. In response to the crisis, the Government has introduced several fiscal rules to ensure fiscal prudence and debt sustainability through new legislations. By learning from the past experience, the Government needs to establish strong monitoring and enforcement mechanisms in relation to recently introduced rule-based fiscal framework to ensure the achievement of fiscal objectives. Establishment of a fiscal council would be useful in this regard, especially to monitor the compliance of the ex-ante and ex-post budget with the fiscal rules. Meanwhile, budgetary allocations should be carefully planned to ensure fiscal rule on primary expenditure is not a deterrent

for growth, especially due to lower spending on capital projects. Moreover, forging ahead with the current fiscal consolidation drive is paramount to comply with the fiscal rules under the PFM Act in the period ahead.

References

- Ardanaz, M., Cavallo, E. & Izquierdo, A., 2023. Challenges and Reform Opportunities for Emerging Markets. IDB Working Paper Series, IDB-WP-1443.
- Ardanaz, M., Cavallo, E., Izquierdo, A. & Puig, J., 2021. Growth-friendly fiscal rules? Safeguarding public investment from budget cuts through fiscal rule design. *Journal of International Money and Finance*, 111(C), pp. 1-17.
- Badinger, H. & Reuter, W., 2017. The case for fiscal rules. *Economic Modelling*, 60(C), p. 334–343.
- Budina, N., Kinda, T., Schaechter, A. & Weber, A., 2013. Chapter 3: Numerical Fiscal Rules: International Trends. In: M. Cangiano, T. Curristine & M. Lazare, eds. *Public Financial Management and Its Emerging Architecture*. Washington, D.C.: International Monetary Fund, pp. 107-135.
- Cordes, T., Kinda, T. & Muthoora, P., 2017. Chapter 12 Expenditure Rules: Effective Tools for Sound Fiscal Policy?. In: V. Gaspar, S. Gupta & M. Carlos, eds. *Fiscal Politics*. Washington D C: International Monetary Fund, 2017, pp. 299-325.
- Davoodi, H, Elger, P., Fotiou, A., Garcia-Macia, D., Han, X., Lagerborg, A., Lam, W. R., & Paulo, M., 2022. Fiscal Rules and Fiscal Councils: Recent Trends and Performance during the COVID-19 Pandemic. IMF Working Paper, Volume WP/22/11.
- International Monetary Fund, 2013. *The Functions and Impact of Fiscal Councils*?. July 2013(063).
- Kopits, G. & Symansky, S., 1998. *Fiscal Rules*. IMF Occasional Paper No. 162.
- Sanchez, T.D., Symansky, S.A., Milesi-Ferretti, G.M., Detragiache, E. & Bella, G.D., 2003. *Rules-Based Fiscal Policy in France, Germany, Italy, and Spain*. IMF Occasional Papers 2003/009.
- Sawadogo, P., 2020. Can fiscal rules improve financial market access for developing countries?. *Journal of Macroeconomics*, 65(C).

Pivotal Role of the Chief Information Security Officer (CISO) in Financial Sector

P G G N Rupasinghe

Senior Assistant Director
Risk Management and Compliance Department

1. Introduction

The landscape of cyber security has significantly evolved over the past decade, with financial institutions being at the forefront of the battle against cyber threats. The role of the Chief Information Security Officer (CISO) has become increasingly crucial as organisations strive to protect sensitive financial data and maintain the trust of their stakeholders. This article delves into the multifaceted role of the CISO, exploring their responsibilities, strategies, and the impact of their work on the overall security posture of financial institutions.

2. The Importance of Cyber Security in Financial Institutions

Financial institutions are prime targets for cyberattacks due to the high value of the data they hold and the critical nature of their services. According to a report by Accenture, financial services firms experience 300 times more cyberattacks than other industries (Accenture, 2021). According to the 2023 Financial Cyber Threat Landscape Report, phishing attacks increased by 30% in the past year, with financial

institutions being the primary targets. (European Union Agency for Cybersecurity, 2022). The consequences of such attacks can be devastating, including financial losses, reputational damage, and regulatory penalties. The increasing frequency and sophistication of cyber threats underscore the importance of having a dedicated CISO to oversee and strengthen the institution's cyber security framework.

2.1. Impact of Cyber Attacks on Financial Institutions

The repercussions of cyber-attacks on financial institutions are profound and multifaceted. Financial losses from such incidents can be staggering, with the average cost of a data breach in the financial sector reaching \$5.85 million in 2022 (IBM Security, 2022). Beyond financial losses, cyber-attacks can erode customer trust, damage reputations, and lead to regulatory fines. The Equifax data breach of 2017 serves as a stark reminder, where personal information of over 147 million consumers was exposed, resulting in significant financial penalties and a long-lasting impact on the company's reputation.

2.2. Importance of Safeguarding Customer Data and Maintaining Trust

In the highly competitive banking sector, customer trust is paramount. Maintaining robust cyber security measures is essential to safeguarding customer data, which in turn fosters trust and loyalty. As highlighted by a 2022 Deloitte survey, 78% of customers are likely to leave a financial institution if it suffers a data breach (Deloitte, 2022). Therefore, investing in strong cyber security frameworks not only protects sensitive data but also sustains customer confidence.

3. Evolution of Cyber Threats

The banking industry has faced cyber threats since the advent of digital banking. Initially, these threats were relatively unsophisticated, primarily involving manual fraud and basic hacking techniques. However, with the proliferation of online banking and digital transactions, cyber threats have evolved significantly. The early 2000s saw the rise of phishing and malware attacks, while the last decade has witnessed more complex threats such as Advanced Persistent Threats (APTs) and targeted ransomware attacks (Symantec, 2022).

3.1. Analysis of Notable Cyber Security Incidents in the Banking Industry

Examining real-world cyber security incidents provides valuable insights into the challenges faced by financial institutions and the effectiveness of their security measures. Notable incidents include:

- The Bangladesh Bank Heist (2016): Cybercriminals used malware to exploit weaknesses in the technical and procedural controls of Bangladesh Bank, resulting in the theft of \$81 million. Although the SWIFT (The Society for Worldwide Interbank Financial Telecommunication) system itself was not compromised, the attackers leveraged

vulnerabilities in the bank's network and security practices to issue unauthorised transactions. This incident highlighted the need for stronger internal security controls and monitoring mechanisms within financial institutions (Reuters, 2016).

- Capital One Data Breach (2019): A misconfigured web application firewall allowed an attacker to access the personal information of over 100 million customers. The breach highlighted the importance of robust access controls, proper firewall configuration, and regular security audits to prevent unauthorised access (Capital One, 2019).
- SolarWinds Supply Chain Attack (2020): In a highly sophisticated operation, attackers infiltrated the software supply chain by compromising SolarWinds' Orion platform, a widely used network management tool. Malicious code was embedded into software updates, which were then unknowingly installed by thousands of organisations, including government agencies, critical infrastructure providers, and financial institutions worldwide. This attack went undetected for months, giving hackers extensive access to sensitive systems and data. The incident underscored the critical need for rigorous supply chain security, continuous monitoring of third-party software, and comprehensive risk management frameworks to protect against similar threats in the future (CISA, 2021).

4. Definition and Responsibilities of a CISO

The Chief Information Security Officer (CISO) is a senior executive responsible for developing and implementing an organisation's information security program. This role encompasses a wide range of responsibilities, including safeguarding the institution's information assets, managing

security technologies, and ensuring compliance with regulatory requirements. A CISO must stay abreast of the latest cyber threats and continuously adapt the organisation's security strategies to mitigate these risks effectively (Gartner, 2022).

5. Placement of the CISO

The CISO's positioning within an organisation directly impacts the effectiveness of its cybersecurity strategy. To protect the organisation's digital assets, the CISO must be strategically placed to influence high-level decisions and ensure security measures are fully integrated into operations.

5.1. Reporting Structure and Organisational Positioning

The reporting structure of the CISO is pivotal. While traditionally reporting to the CIO, this can limit the CISO's ability to prioritise security. Ideally, the CISO should report directly to the CEO or Board, giving them the authority to align cybersecurity with organisational strategy, advocate for necessary investments, and provide updates on emerging threats. This visibility ensures cybersecurity is a top priority. Without such access, the CISO may find it challenging to secure the resources needed to effectively address cybersecurity concerns.

5.2. Independence and Authority

A CISO with a high level of authority and independence is better positioned to make decisions that prioritise security over short-term business goals. This autonomy enables the CISO to enforce security protocols, even when they may conflict with other business priorities. Without sufficient authority, CISO might struggle to implement policies or enforce necessary changes, especially when faced with internal resistance from departments more focused on business outcomes than security. CISO's role should not be undermined by conflicting interests within the

organisation. The placement of the CISO must reflect their pivotal role as the primary steward of organisational cybersecurity, ensuring they have the necessary power to act decisively in times of crisis.

5.3. Alignment with Business and Risk Management

While the CISO must maintain independence, it is also essential that they work closely with other business functions. The position of the CISO should allow them to collaborate effectively with departments like IT, Legal, Risk Management and Compliance to ensure cybersecurity is woven into every facet of the organisation's operations. For example, a CISO involved in strategic business decisions can help mitigate cybersecurity risks before they become major threats, rather than reacting after an incident occurs.

In organisations where cybersecurity is integrated into broader risk management frameworks, the CISO can help identify and address both operational and strategic risks that affect the company's ability to meet its objectives. This ensures that cybersecurity efforts are not isolated from the organisation's core goals but rather support the business's long-term success and resilience.

5.4. Impact on Cybersecurity Culture

The placement of the CISO also has a significant impact on the organisation's cybersecurity culture. A CISO with direct access to the board and senior management can promote a security-first mindset across all levels of the organisation. This cultural shift is vital, as a robust cybersecurity culture can help prevent incidents before they occur, as employees are more likely to be vigilant and adhere to security protocols.

Conversely, when the CISO is buried within lower levels of the organisation or in departments not closely linked to strategic decisions, the

focus on cybersecurity may diminish, reducing its effectiveness. It is therefore crucial that the placement of the CISO reflects the importance of cybersecurity in an organisation's broader operational and strategic priorities.

6. The Evolving Role of the CISO

The role of the CISO has evolved from being primarily focused on IT security to encompassing a broader range of responsibilities that include risk management, regulatory compliance, and strategic planning. This evolution reflects the growing recognition that cyber security is not just an IT issue but a critical component of overall business strategy.

6.1. The Strategic Role of the CISO in an Organisation

A key responsibility of the CISO is to develop and implement a comprehensive cyber security strategy that aligns with the organisation's overall business objectives. This involves identifying potential threats, assessing vulnerabilities, and deploying robust defense mechanisms. CISO must stay abreast of the latest trends and developments in cyber security to ensure that the institution's defenses remain effective against emerging threats. CISO must work closely with other senior leaders to integrate cyber security into the organisation's strategic planning processes and ensure that security considerations are embedded in every aspect of the business.

According to the International Monetary Fund (IMF), effective cyber risk management is essential for the stability of the financial system (IMF, 2023).

6.2. Creating and Implementing a Comprehensive Cyber Security Plan

One of the primary responsibilities of CISO is to develop and implement a comprehensive cyber security plan. This plan should encompass

all aspects of the organisation's cyber security posture, from threat detection and prevention to incident response and recovery. Key components of a robust cyber security plan include:

- Regular risk assessments to identify and mitigate potential vulnerabilities.
- Deployment of advanced security technologies such as intrusion detection systems, firewalls, and encryption.
- Employee training and awareness programs to foster a security-conscious culture.
- Continuous monitoring and evaluation of security measures to ensure their effectiveness.
- Policy development and enforcement to maintain cybersecurity standards and regulatory compliance.
- Incident response and crisis management to rapidly detect, contain, and recover from security incidents.
- Data protection and privacy management to safeguard sensitive data in line with privacy laws.
- Third-party and supply chain risk management to secure vendor relationships and mitigate external risks.
- Disaster recovery and business continuity planning (BCP) to ensure swift operational recovery post-incident.
- Threat intelligence and analysis to proactively address emerging security threats.
- Compliance and audit management to meet regulatory, legal, and contractual requirements.

6.3. Collaboration with Other Departments (IT, Legal, Risk Management, Compliance, etc.) and communication

Collaboration is another vital component of

CISO's role. Cyber security is not an isolated function but requires coordination with various departments, including IT, legal, risk management and compliance. The CISO must work closely with these departments to ensure a cohesive and comprehensive approach to cyber security. The Financial Stability Board (FSB) recommends that CISOs also engage with external stakeholders, including industry peers and regulatory bodies, to share intelligence and best practices (FSB, 2023). Effective communication is essential for ensuring that all stakeholders are aware of the organisation's cyber security posture and any potential risks. Regular cross-departmental meetings and communication channels are essential for maintaining alignment and addressing any security-related issues promptly (SANS Institute, 2022).

6.4. Risk Assessment and Management

Risk assessment and management are the core components of CISO's responsibilities. This involves identifying potential risks, assessing their impact on the organisation, and implementing appropriate controls to mitigate these risks. A robust risk management framework should include:

- Regular vulnerability assessments and penetration testing to identify weaknesses.
- Risk assessment methodologies to evaluate the potential impact and likelihood of different threats.
- Implementation of risk mitigation strategies such as network segmentation, access controls, and data encryption.
- Development of a risk management plan that outlines the organisation's risk tolerance and response strategies.

(ENISA) emphasises that effective risk management practices can significantly reduce the impact of cyber incidents (ENISA, 2022).

6.5. Establishing an Incident Response Plan

An effective incident response plan is critical for minimising the impact of cyber security incidents. The CISO is responsible for developing and maintaining this plan, which should include detailed procedures for detecting, responding to, and recovering from security incidents. Key elements of an incident response plan include:

- Incident detection and analysis procedures to quickly identify and assess the nature of the threat.
- Incident response team roles and responsibilities to ensure a coordinated and efficient response.
- Communication protocols for internal and external stakeholders.
- Post-incident analysis and reporting to identify lessons learned and improve future response efforts (ENISA, 2022).

6.6. Leading the Response to Cyber Security Incidents

In the event of a cyber security incident, CISO takes on a leadership role in managing the response. This involves coordinating with the incident response team, communicating with executive leadership, and ensuring that appropriate actions are taken to contain and mitigate the threat. The CISO must also oversee the investigation process to determine the root cause of the incident and implement measures to prevent similar incidents in the future (Verizon, 2023).

6.7. Recovery and Post-Incident Analysis

Recovery from a cyber security incident involves restoring affected systems and data, as well as addressing any vulnerabilities that were exploited.

The CISO plays a crucial role in overseeing the recovery process and ensuring that normal operations are resumed as quickly and securely as possible. Additionally, post-incident analysis is essential for identifying any gaps in the organisation's security posture and implementing improvements to prevent future incidents. This process should include a thorough review of the incident response and recovery efforts, as well as a detailed report outlining the lessons learned and recommended actions.

6.8. Regulatory Compliance

The banking and financial services industry operates within a complex landscape of regulatory frameworks and compliance standards designed to ensure the security, privacy, and integrity of financial systems. These frameworks not only establish mandatory requirements but also encourage voluntary adherence to best practices that strengthen organisational resilience against cyber threats. Key regulatory and compliance components include, but are not limited to, the following:

- ISO Standards (ISO/IEC 27001, ISO/IEC 27701, ISO/IEC 31000), which provide a comprehensive framework for information security management, privacy information management, and risk management to ensure organisational resilience and data protection (ISO, 2022).
- The Basel Committee on Banking Supervision's principles for the sound management of operational risk, which include specific guidelines for cyber security (Basel Committee on Banking Supervision, 2021).
- The Gramm-Leach-Bliley Act (GLBA), which requires financial institutions in the United States to protect the confidentiality

and integrity of customer information (Federal Trade Commission, 2022).

- The Personal Data Protection Act (PDPA), which regulates the processing of personal data, strengthens the rights of data subjects, and establishes the Data Protection Authority to safeguard privacy and ensure compliance with data protection standards (Data Protection Authority Sri Lanka, 2022).
- The Payment Card Industry Data Security Standard (PCI DSS), which sets forth requirements for securing payment card data (PCI Security Standards Council, 2022).
- The General Data Protection Regulation (GDPR), which mandates strict data protection and privacy measures for organisations operating within the European Union (European Union, 2022).
- The SWIFT Customer Security Programme mandates specific cybersecurity controls for institutions that use SWIFT's global payment messaging network. Compliance is essential for protecting against fraudulent transactions and ensuring secure messaging within the global financial ecosystem (SWIFT Customer Security Programme, 2024).
- Further, National Institute of Standards and Technology (NIST) provides a comprehensive Cybersecurity Framework for organizations to manage and reduce cybersecurity risks (NIST, 2022). Center for Internet Security (CIS) offers a set of best practices and security controls for securing IT systems and protecting sensitive data (CIS, 2022) and Open Web Application Security Project (OWASP) provides guidelines for securing web and mobile applications by identifying and mitigating vulnerabilities (OWASP, 2022).

CISO must ensure that the organisation complies with all relevant regulatory requirements. Non-compliance can result in significant fines and legal repercussions. The Financial Stability Board (FSB) recommends that CISOs stay informed about the latest regulatory changes and work closely with regulatory bodies to ensure compliance (FSB, 2023).

6.9. Building a Security Conscious Culture

Human error remains one of the leading causes of security breaches. A report by Cybersecurity Ventures estimates that human error accounts for 95% of all cyber security breaches (Cybersecurity Ventures, 2024). CISO plays a critical role in fostering a culture of cyber security within the organisation. This includes developing and implementing employee training and awareness programs to educate staff about the importance of cyber security and the role they play in protecting the organisation's assets. By promoting a security-conscious culture, the CISO can reduce the risk of breaches caused by human error.

7. Challenges Faced by CISOs

Despite the critical importance of their role, CISOs face numerous challenges in executing their responsibilities effectively. Some of the key challenges include:

7.1. Rapidly Evolving Threat Landscape

The cyber threat landscape is constantly evolving, with new threats emerging regularly. This requires CISOs to continuously update their knowledge and adapt their strategies to address these new threats. Staying ahead of cybercriminals is a significant challenge that requires constant vigilance and innovation.

7.2. Resource Constraints

Many financial institutions face resource constraints that can limit their ability to implement

comprehensive cyber security measures. This includes budget limitations, staffing shortages, and limited access to advanced security technologies. CISOs must find ways to work within these constraints to develop effective security strategies.

7.3. Balancing Security and Business Objectives

CISOs must strike a delicate balance between ensuring robust security and supporting the organisation's business objectives. Overly stringent security measures can hinder business operations and innovation, while insufficient security can expose the organisation to significant risks. Finding the right balance is a critical challenge for CISOs.

7.4. Regulatory Complexity

Navigating the complex regulatory landscape can be challenging for CISOs. Different jurisdictions have different regulatory requirements, and ensuring compliance with all applicable regulations can be a daunting task. CISOs must stay informed about the latest regulatory changes and ensure that their organisations comply with all relevant requirements.

8. Strategies for Effective Cyber Security Management

To address these challenges and effectively manage cyber security, CISOs can adopt several key strategies:

8.1. Continuous Monitoring and Threat Intelligence

Continuous monitoring and threat intelligence are essential for staying ahead of emerging threats. CISOs should implement advanced monitoring tools to detect and respond to threats in real time. Additionally, leveraging threat intelligence from various sources can provide valuable insights into potential threats and help the organisation take proactive measures to mitigate them.

8.2. Adopting a Risk-Based Approach

A risk-based approach to cyber security focuses on identifying and prioritising the most critical risks to the organisation. This involves conducting regular risk assessments to identify vulnerabilities and assess their potential impact. By prioritising the most significant risks, CISOs can allocate resources more effectively and develop targeted strategies to address them.

8.3. Implementing Layered Security Measures

A layered security approach involves implementing multiple layers of security controls to protect the organisation's assets. This includes technical controls such as firewalls, intrusion detection systems, and encryption, as well as administrative controls such as policies, procedures, and employee training. By implementing a multi-layered defense strategy, CISOs can enhance the organisation's overall security posture.

8.4. Engaging in Industry Collaboration

Collaboration with industry peers and regulatory bodies is essential for sharing intelligence and best practices. CISOs should participate in industry forums, join cyber security working groups, and engage with regulatory bodies to stay informed about the latest trends and developments. Collaboration can also help CISOs build a network of trusted partners who can provide support in times of crisis.

8.5. Investing in Cyber Security Talent

Building a skilled and knowledgeable cyber security team is critical for effective cyber security management. CISOs should invest in hiring and retaining top talent, as well as providing ongoing training and development opportunities for their teams. By building a strong cyber security team, CISOs can ensure that their organisations are well-equipped to handle emerging threats.

9. Case Studies and Best Practices

To illustrate the impact of effective cyber security management, this section presents several case studies and best practices from leading financial institutions.

9.1. Case Study: JPMorgan Chase

JPMorgan Chase is one of the largest and most prominent financial institutions in the world. The company has made significant investments in cyber security, with an annual budget of over \$600 million dedicated to protecting its assets. The CISO at JPMorgan Chase has implemented a comprehensive cyber security strategy that includes continuous monitoring, threat intelligence, and employee training programs. As a result, the company has been able to detect and respond to threats more effectively, reducing the impact of cyber incidents (JPMorgan Chase, 2021).

9.2. Case Study: HSBC

HSBC is another leading financial institution that has prioritised cyber security. The company's CISO has implemented a risk-based approach to cyber security, focusing on identifying and mitigating the most critical risks. HSBC has also invested in advanced security technologies, such as artificial intelligence and machine learning, to enhance its threat detection capabilities. By adopting a proactive approach to cyber security, HSBC has been able to strengthen its defenses and protect its customers' data (HSBC USA Inc, 2024).

9.3. Best Practice: Employee Training and Awareness Programs

One of the most effective ways to mitigate the risk of security breaches caused by human error is to implement comprehensive employee training and awareness programs. Financial institutions such as Goldman Sachs and Bank of America have developed extensive training programs to

educate their employees about cyber security best practices and the role, they play in protecting the organisation's assets. These programs include regular training sessions, phishing simulations, and awareness campaigns to reinforce the importance of cyber security.

9.4. Best Practice: Incident Response Planning

Having a well-defined incident response plan is critical for effectively managing cyber security incidents. Financial institutions such as Citibank and Wells Fargo have developed robust incident response plans that outline the steps to be taken in the event of a security breach. These plans include procedures for identifying and containing the breach, notifying affected stakeholders, and conducting post-incident analysis to identify areas for improvement. By having a clear and actionable incident response plan, these institutions can respond to incidents more effectively and minimise their impact.

10. The Future of CISO's role in Financial Institutions

As the cyber threat landscape continues to evolve, the role of CISO will become increasingly important. Future trends in cyber security are likely to include the following:

10.1. Increased Use of Artificial Intelligence and Machine Learning

Artificial intelligence (AI) and machine learning (ML) technologies are playing an increasingly significant role in cyber security. These technologies can help organisations detect and respond to threats more quickly and accurately. According to a report by Gartner, AI and ML will be essential for enhancing threat detection and response capabilities (Gartner, 2023). CISOs will need to stay informed about the latest advancements in these technologies and explore ways to integrate them into their cyber security strategies.

10.2. Greater Emphasis on Data Privacy

Data privacy will continue to be a significant concern for financial institutions. The introduction of new data privacy regulations, such as the California Consumer Privacy Act (CCPA) and the GDPR, has highlighted the importance of protecting customer data. CISOs will need to ensure that their organisations comply with these regulations and implement measures to safeguard customer information.

10.3. Expansion of Cyber Security Talent

The demand for skilled cyber security professionals is expected to continue growing. According to the (ISC)² Cybersecurity Workforce Study, there is a global shortage of over 3 million cyber security professionals (ISC)², 2023). CISOs will need to invest in building and retaining a strong cyber security team to address this talent gap and ensure that their organisations are well protected.

10.4. Increased Collaboration and Information Sharing

Collaboration and information sharing will be critical for staying ahead of emerging threats. Financial institutions will need to work closely with industry peers, regulatory bodies, and government agencies to share intelligence and best practices. CISOs will play a key role in fostering these collaborative efforts and ensuring that their organisations benefit from shared knowledge and insights.

10.5. Adoption of Zero Trust Architecture

Zero Trust Architecture (ZTA) is an emerging security model that emphasises the importance of verifying the identity of users and devices before granting access to resources. According to Forrester Research, Zero Trust principles will become increasingly important for securing

financial institutions (Forrester, 2023). CISOs will need to explore the adoption of ZTA to enhance their organisation's security posture and protect against unauthorised access.

11. Conclusion

The role of the Chief Information Security Officer is critical in the modern financial landscape, where cyber threats are increasingly sophisticated and prevalent. By developing robust strategies, managing risks, fostering a security-conscious culture, and promoting collaboration, CISOs play a vital role in defending financial institutions against cyber threats. Despite the challenges they face, CISOs can effectively manage cyber security by adopting key strategies such as continuous monitoring, a risk-based approach, layered security measures, industry collaboration, and investing in cyber security talent.

As the cyber threat landscape continues to evolve, CISOs will need to stay informed about the latest trends and developments, including advancements in AI and ML, data privacy regulations, the expansion of cyber security talent, increased collaboration, and the adoption of Zero Trust Architecture. By staying ahead of these trends and continuously adapting their strategies, CISOs can ensure that their organisations remain resilient and secure in the face of ever-changing cyber threats.

References:

1. Accenture (2021) *The Cost of Cybercrime*. Available at: <https://www.accenture.com/us-en/insights/security/cost-cybercrime-study>
2. Basel Committee on Banking Supervision (2021) *Revisions to the Principles for the Sound Management of Operational Risk*. Available at: <https://www.bis.org/bcbs/publ/d515.pdf>
3. Capital One (2019) *Capital One Announces Data Security Incident*. Available at: <https://www.capitalone.com/about/newsroom/capital-one-announces-data-security-incident>
4. Center for Internet Security (CIS) (2022) *CIS Controls*. Available at: <https://www.cisecurity.org/controls>
5. Cybersecurity and Infrastructure Security Agency (CISA) (2021) *Remediating the SolarWinds and Active Directory/M365 Compromise*. Available at: <https://www.cisa.gov/remediating-solarwinds-and-active-directorym365-compromise>
6. Cybersecurity Ventures (2024) *Cybersecurity Statistics and Facts*. Available at: <https://cybersecurityventures.com>
7. Data Protection Authority Sri Lanka (2022) *Personal Data Protection Act, No. 9 of 2022*. Available at: <https://www.dpa.gov.lk>
8. Deloitte (2022) *The Deloitte Consumer Privacy Study*. Available at: <https://www2.deloitte.com/us/en/insights/industry/financial-services/global-privacy-study.html>
9. European Union (2022) *General Data Protection Regulation (GDPR)*. Available at: <https://gdpr.eu>
10. European Union Agency for Cybersecurity (ENISA) (2022) *Threat Landscape 2022*. Available at: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022>
11. Federal Trade Commission (2022) *Gramm-Leach-Bliley Act*. Available at: <https://www.ftc.gov/enforcement/statutes/gramm-lea>
12. Financial Stability Board (FSB) (2023) *Effective Practices for Cyber Incident Response and Recovery*. Available at: <https://www.fsb.org/2023/01/effective-practices-for-cyber-incident-response-and-recovery>
13. Forbes Advisor (2024) *Cybersecurity Statistics and Facts*. Available at: <https://www.forbes.com/advisor/education/it-and-tech/cybersecurity-statistics>

14. Forrester Research (2023) *Zero Trust Extended Ecosystem Platform Providers*. Available at: <https://www.forrester.com/report/the-forrester-wave-zero-trust-extended-ecosystem-platform-providers-q2-2023/RES157638>
15. Gartner (2022) *Top Trends in Cybersecurity*. Available at: <https://www.gartner.com/en/doc/761902-gartner-top-trends-in-cybersecurity-2022>
16. Gartner (2023) *Top Trends in Cybersecurity*. Available at: <https://www.gartner.com/en/doc/761902-gartner-top-trends-in-cybersecurity-2023>
17. HSBC USA Inc. (2023) *Form 10-K Annual Report for the fiscal year ended December 31, 2023, to U.S. Securities and Exchange Commission (SEC)*. Available at: <https://www.sec.gov/Archives/edgar/data/83246/000008324624000004/hsbcusa-20231231.htm>
18. IBM Security (2022) *Cost of a Data Breach Report 2022*. Available at: <https://www.ibm.com/security/data-breach>.
19. International Monetary Fund (IMF) (2023) *Cyber Risk Supervision and the IMF's Role*. Available at: <https://www.imf.org/en/Publications/WP/Issues/2023/03/01/Cyber-Risk-Supervision-and-the-IMFs-Role-521999>
20. ISC² (2023) *Cybersecurity Workforce Study*. Available at: <https://www.isc2.org/Research/Workforce-Study>
21. ISO (2022) *ISO/IEC 27001, ISO/IEC 27701, ISO/IEC 31000*. Available at: <https://www.iso.org>
22. JPMorgan Chase (2021) *Annual Report*. Available at: [https://www.jpmorganchase.com/content/dam/](https://www.jpmorganchase.com/content/dam/jpmc/jpmorgan-chase-and-co/investor-relations/documents/annualreport.pdf)
23. National Institute of Standards and Technology (NIST) (2022) *Cybersecurity Framework*. Available at: <https://www.nist.gov/cyberframework>
24. Open Web Application Security Project (OWASP) (2022) *OWASP Top Ten*. Available at: <https://owasp.org/www-project-top-ten>
25. PCI Security Standards Council (2022) *Payment Card Industry Data Security Standard (PCI DSS) Requirements and Security Assessment Procedures*. Available at: https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf
26. Reuters (2016) *Exclusive - Bangladesh Bank hackers compromised SWIFT software, warning issued*. Available at: <https://www.reuters.com/article/world/exclusive-bangladesh-bank-hackers-compromised-swift-software-warning-issued-idUSKCN0XM0DW>
27. SANS Institute (2022) *SANS 2022 SOC Survey: Optimizing SOC Operations and Collaboration*. Available at: <https://www.sans.org/white-papers/sans-2022-soc-survey>
28. SWIFT (2024) *Customer Security Programme (CSP)*. Available at: <https://www2.swift.com/knowledgecentre/products/Customer%20Security%20Programme>
29. Symantec (2022) *Internet Security Threat Report*. Available at: <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/internet-security-threat-report-2022>
30. Verizon (2023) *Data Breach Investigations Report 2023*. Available at: <https://www.verizon.com/business/resources/reports/dbir>

Collaboration and Knowledge Sharing in Cyber Security



S P E S Jayarathne, Management Assistant (Senior), Facility Management Department

Introduction

The word “cyber” means “related to computers or computer networks (internet).” Therefore, cyber security is simply protection of your computer and the information on the computer from malicious attacks. Without cyber security, data on a computer can be erased, modified or stolen. Cyber Security is the effort towards protection of IT assets from attacks, damages or unauthorized access through technological solutions as well as non-technological best practices.

Cyber Security is the responsibility of everyone in an organization. Awareness of cyber security reduces institutional and personal risk by changing the culture, behavior and ethics. It helps to understand the risk of using current technology and how to defend against cyber threats, both at work and at home effectively.

The hacking takes place for financial gain, as a hobby, to revenge, to leak information, hacktivism for politically or socially motivated purposes and for security reasons.

Pakistan is facing more cyber security threats than Sri Lanka.

Famous Cyber Attacks

In Bangladesh Bank incident in Pakistan the hackers misspelled “Foundation” in their request to transfer the funds, spelling the word as “Fundation”. This spelling error gained suspicion from Deutsche Bank, a routing bank which put a halt to the transactions by questioning after seeking clarifications from Bangladesh Bank.

In Iran, Stuxnet is a computer worm discovered in June 2010. It initially spread via Microsoft Windows, and targeted Siemens industrial software

and equipment. Then took control of functions of a nuclear power plant too.

On November 24, 2014, a hacker group which was identified itself by the name “Guardians of Peace” (GOP) leaked confidential data from the film studio Sony Pictures. The data included personal information about Sony Pictures employees and their families, e-mails between employees, information about executive salaries at the company and copies of the non-released Sony films. Multiple reports suggested that the attack is tied to the North Korean government, who expressed outrage over the Sony-backed film “The Interview,” an action-comedy centered on an assassination plot against North Korean leader Kim Jong Un.

Some other most notable cyber security breaches were Uber, Equifax, Yahoo and LinkedIn.

Uber : 57 million user accounts were hacked in 2016. Uber paid two hackers to destroy the stolen data. Damage was Uber fired chief security officer Joe Sullivan and his deputy. Company valuation dropped by 30 percent.

Equifax (consumer credit rating agency) : 143 million records of personal information were hacked. The leaked data included names, social security numbers, birth dates, addresses and driver’s license numbers. Damages were CEO, CIO and CISO resigned immediately after the news broke and stock prices slumped by 35 percent in a week. Third-quarter in 2017, profit declined by 27 percent compared with last year and the company has incurred \$87 million in cost related to the breach.

Yahoo : 3 billion user accounts were hacked in 2013. Number wasn’t disclosed until October 2017. Damage was Yahoo has faced 41 class action lawsuits.

LinkedIn: 117 million user accounts were hacked in 2012. The scale of the breach reported first 6.5 million. The actual number was found when a Russian hacker began selling 117 million emails and passwords for bitcoin on a dark web market place in May 2016. Damage was a group of LinkedIn Premium users filed a class action against LinkedIn for failing to protect user data.

In 2018, Facebook announced the largest breach in the company’s history. The breach affected about 50 million of users, allowing hackers to take over their accounts.

In 2015, several parts of Ukraine witnessed blackout. Information systems of 3 power distribution companies were compromised. Hackers had used phishing emails to hack the power distribution companies.

Causes of compromised security are lack of security awareness, human errors, malicious/pirated software, lost/ stolen computers, disgruntle employees and insufficient funding.

Types of Cyber Attacks and How to Avoid them.

Social engineering, phishing, malware, password cracking, wireless access, identity theft, insider threat and ransomware can be recognized as most prominent security threats and attacks.

Social Engineering

A company can spend hundreds of thousands of dollars on firewalls, detection systems and other security technologies. But an attacker can call one trusted person within the company. If that person compromises and the attacker gets in, all the money spent on technology is essentially wasted.

Social Engineering is an art of convincing people to reveal sensitive / confidential information by

deceiving and manipulating them. Criminals try to trick people in a way that they disclose information, download malware and perform unauthorized transactions. It is much easier to fool someone into giving their password rather than hacking them.

Vishing Attacks

Vishing is the telephone equivalent of phishing. It is described as the act of using the telephone in an attempt to scam the user into surrendering private information that will be used for identity theft.

Here are some tips to help you to avoid vishing attacks. Think before you speak. Scammers want you to act and give out information. Have your guard up with automated calls. Be aware that caller ID can be easily spoofed by scammers. Verify phone numbers before calling back and better not to answer the unknown numbers. Use a different phone to call back. Do not share your card details, NIC and passport credentials over a phone call. Further, do not believe sweet words and use blocking apps when it is necessary.

Phishing Attacks

Phishing is an illegal attempt to acquire sensitive information, such as usernames, passwords and financial data (debit / credit card information, etc.). Phishing is done for malicious reasons, by impersonating a trustworthy entity in an electronic communication. Think Before you Click!. Types of motivations in phishing are greed, fear, curiosity, sympathy and respect for authority.

There is NO PATCH to human negligence.

Malware

It is an abbreviated term meaning “malicious software”. It damages a computer without the knowledge of the owner. That means it disrupts the

computer operation, gather sensitive information and gain access to computer. Accepting files and downloads without checking properly about the source, opening infected e-mail attachments, installing pirated software, not updating or installing new versions/updates and not running the latest/updated anti-malware program are means to get a computer infected.

A malware attack indicates unusual computer behavior, slow performance, computer freezing frequently, files and folders go missing, appearing of unknown files/ folders, fake anti-virus alerts, changed drive label, filenames & file sizes etc.

When the antivirus is switched off, it would be fake antivirus warnings, password not working, increasing number of friends on social media, appearing new icons on dashboard, cursor moving on its own, redirection to different websites, folders and files go missing, personal data is on internet even though you didn't put there, unusual behavior of webcam and computer is working slowly.

When there is a malware, first you should install a reliable antivirus and scan, delete all unfamiliar programs, change the passwords of all accounts and report to IT specialist in relevant authority.

Password Cracking

Password cracking techniques are used to recover passwords with the purposes such as gaining access to sensitive data, financial information or personal accounts from computer systems. Key loggers, password guessing, phishing, shoulder surfing, social engineering and brute-force / dictionary attack are the most used password cracking methods.

Most attacks are successful due to weak or easily guessable passwords. When creating a secure

password always use unique, lengthy & strong/complex, at least 8 character password with combination of alphabets, numbers and special characters (*, %, @, #, \$, ^). Use passwords that can be easily remembered and significantly different from earlier. Use different passwords for different accounts. Change password regularly as per policy. Change passwords whenever you suspect a compromise. Block accounts on a number of failed attempts.

Identity Theft

Identity theft is the deliberate use of someone else's identity. Stealing other's personal and financial data, gaining other benefits by pretending to be someone else, wrongfully obtaining and using another person's personal or financial data in a way that involves fraud or deception, typically for financial gain.

Identity theft is a process of stealing someone's identity information and misusing the information to accomplish attacker's goals for fraudulent purposes such as committing theft and crimes. (Eg. using someone else's N.I.C. to register).

Google knows about every step you take, every search you make, every word you say, every tab you view, every clip you watch and every app you use.

To minimize the risk, secure personal information both at workplace and home, cross check and review financial accounts, bank statements and credit reports regularly, secure or shred confidential documents, don't respond unsolicited requests, secure sensitive information, pay attention to billing cycles, collect mail and promptly use antivirus & firewall.. Never provide your personal information to others and unsubscribe from unnecessary email services.

ATM Skimming

ATM skimming is a way of stealing PINs and other information off credit cards and debit cards by rigging machines with hidden recording devices.

On October 27, 2018 customers of the Bank Islami in Pakistan received automated messages about transactions from their payment cards. The money had been withdrawn from different locations in USA, Russia and other countries. Bank Islami issued a circular stating that, all funds withdrawn from the accounts (i.e. Rs. 2.6 Million) of customers have been reversed. However, ATM skimming, social engineering and system breach (Hackers infiltrated into a Bank's secure system) may be some reasons for the same.

Two Chinese men had been arrested by Police in Karachi on charges of installing skimming devices in ATMs. This was not the first time that someone had tried to hack ATMs in Pakistan. Last year HBL reported that over 559 customers' accounts were compromised by hackers and over Rs 10 million were stolen from them.

As an example, for card skimming, a shop assistant takes your card out of your sight in order to process your transaction. You are asked to swipe your card through more than one machine. You notice something suspicious about the card slot on an ATM (e.g. an attached device) and you notice unusual or unauthorized transactions on your account or credit card statement.

Ransomware

Ransomware is a type of malware that hackers install on your computer or mobile device without your consent or knowledge. It encrypts files on your computer or mobile device.. It then communicates with user via pop-up messages and restrict access

to computer or mobile device until the required ransom is paid.

Don't be a victim of data and financial loss. Usually ransomware enters a network and computers through emails with malicious attachments. Once the user opens the attached file, a malicious software is installed unknowingly on the system. This malicious software blocks access to the system, until the hackers receive money.

Information Security is Everyone's Responsibility.

Some Misconceptions are, there's nothing important on my computer, we have virus software so my computer is protected from everything, all threats are from the outside, it's not my job to worry about security, technology provides full protection and downloading PDF documents is secure, information security is the responsibility of IT etc.

Most common mistakes are poor password management, workstation attached and unattended, malicious e-mail attachments, ineffective anti-virus software, uncontrolled laptops, unreported security violations, casual use of mobile phones and apps, updates, hot fixes, service packs not installed and poor perimeter protection (electronic and physical).

For clean desk and secure workspace, use locked cabinets/drawers for sensitive information on printable media and portable storage media. When left unattended, lock/log-off before leaving the desk. Secured discussion rooms must be used for sharing and discussing sensitive information.

Proper document disposal using paper shredders and burn bins and preventing dumpster diving information leaks. Be discreet in open areas. Report theft immediately to local authorities and protect your devices while travelling. ID cards and perhaps uniforms along with other access control measures should be protected. Employ trained security personnel supported by surveillance cameras, alarm systems etc. Critical areas of organization must be restricted to prevent unauthorized access. Visitors should be escorted into visitor rooms or lounges by office security or personnel. Supervised access must be ensured for janitorial or other working staff to office areas containing sensitive information.

To protect your kids from online, educate them about cyberbullying. Have a dedicated home computer just for your kids. Monitor their online activities. Establish basic ground rules on online use. Don't share too much private information via online.

Security events and incidents should be reported to limit the damage, reduce the cost of recovery and negative consequences, safe environment and enhancement of awareness.

Finally, cyber security is responsibility of everyone in the organization. IS team can only enforce, the culture for cyber security evolves from within the organization. Every employee is important as they play key roles towards ensuring that its organization is protected. Think Before You Click at office and at home.

Strengthening Legal Framework applicable for Licensed Banks: Amendments to the Banking Act



W G N P Kumari, Deputy Director, Bank Supervision Department

Introduction

The Central Bank of Sri Lanka (CBSL), being the apex financial institution in Sri Lanka, has a statutory responsibility of preserving the financial system stability of the country. In terms of the Central Bank of Sri Lanka Act No.16 of 2023, the primary object of CBSL is to achieve and maintain domestic price stability and other object is to secure the financial system stability. Further in terms of the Section 61 of the cited Act, CBSL is the exclusive authority for regulation, licensing, registration, and supervision of financial institutions in Sri Lanka.

Banking Sector accounts for nearly 62% of the total assets of the financial sector and consist of 24 licensed commercial banks (includes 2 state owned banks, and 11 banks incorporated outside Sri Lanka) and 6 licensed specialised banks. As of 30 September 2024, total assets of the banking sector were Rs. 21.2 trillion with deposits of Rs.17.3 trillion and Rs.11.3 trillion of loans and advances. Banking sector is mainly funded by the depositors' funds, and it is essential to safeguard the interest of depositors and other stakeholders and maintain their confidence in the banking system. CBSL, with a view to preserving the safety and soundness of the banking sector continuously engages in

strengthening its legal and regulatory framework pertaining to licensed banks and initiates proactive measures to discharge its statutory responsibilities.

Amendments to the Banking Act No.30 of 1988

The Banking Act No.30 of 1988, as amended (BA), is the key legislation pertaining to licensing, and regulating of persons carrying on banking business and controlling of matters relating to such licensed banks. BA was lastly amended in 2006 and with the current regulatory and market developments and changes in the international best practices of banking, CBSL initiated necessary measures to amend BA. This initiative was endorsed by the International Monetary Fund, by setting a structural benchmark under the Extended Fund Facility Programme with the other key regulatory reforms relating to the financial sector. The Core Principles for Effective Banking Supervision issued by the Basel Committee for Banking Supervision which set the minimum standard for sound prudential regulation and supervision of banks were also factored as appropriate in amending the Banking Act.

Accordingly, Banking (Amendment) Bill was passed by the Parliament in April 2024 and came

into operation with effect from 15 June 2024 as the Banking (Amendment) Act No.24 of 2024.

Key Amendments to the Banking Act

The following key amendments to the Banking Act were introduced via the Banking (Amendment) Act No.24 of 2024.

i. Minimum Licensing Requirements: In addition to the documentary requirements in the Act, new criteria were introduced for eligibility to apply for a bank licence, including minimum entry capital requirements, nature and adequacy of financial resources, suitability of the key shareholders, fitness and propriety of Directors, Chief Executive Officer (CEO), Key Management Personnel (KMP), transparency of ownership structure and beneficial ownership of the applicant.

ii. Shareholder Suitability: A new provision has been introduced for assessing the suitability of shareholders for the purpose of granting approval for the acquisition of a material interest (i.e., over 10% of the issued capital carrying voting rights) in a licensed commercial bank (LCB). In this regard, CBSL may consider *inter alia* the nature and sufficiency of financial resources, soundness and feasibility of the business plans, business track record and experience, transparency of the ownership structure and beneficial ownership of the applicant.

iii. Subsidiarization of Foreign Banks: At present, foreign banks are operating in Sri Lanka as branches. Therefore, a new provision has been introduced specifying that branches of foreign banks entering Sri Lanka in future to be incorporated either as a subsidiary or

to operate as a branch. Further, CBSL was empowered to require subsidiarization of any existing foreign bank considering *inter alia* the soundness of the financial position, risk management, governance structure, capital adequacy, and the availability of liquidity.

iv. Bank Ownership: In terms of the BA, an individual, partnership or corporate body shall not, either directly or indirectly or through a nominee or acting in concert with any other individual, partnership or corporate body, acquire a material interest of an LCB without the prior written approval of the Governing Board with the concurrence of the Minister. The definition of “material interest” was expanded to capture the concept of “significant influence” where CBSL may determine that there exists a significant influence over the LCB to nominate, appoint or remove a director, CEO or KMP of an LCB or to exercise control over policies pursuant to a contract or otherwise. In addition, strengthened measures were introduced for breaches of the provisions on acquisition of material interest such as to suspend the exercise of voting rights entitled to such shareholding, dispose or sell shares within a specified time, non-accrual of dividends for such shares, and prohibit payment of any aum including any form of distribution.

v. Acquisitions, Mergers, and Consolidation: Amendments have been introduced enabling an LCB to acquire the business or part of the business of a licensed finance company (LFC) as well as for an LCB to sell all or part of its business. Further, LCBs have also been permitted to merge or consolidate with an LFC. Further, a provision has been added to enable the acquisition of

the business or part of the business of another financial institution subject to the regulation or supervision of CBSL.

vi. Disposal of Non-Financial Subsidiaries:

With a view to enabling banks to focus on their banking business and allocating resources effectively to the licensed bank, provision has been added where LCBs are required to divest ownership of non-financial subsidiaries that do not provide services to the licensed bank or its banking group. A transitional period of 05 years has been granted in this regard.

vii. Consolidated Supervision: As per the amendments, CBSL was empowered to examine LCBs on a solo or consolidated basis including its subsidiaries.

viii. Proportionality: CBSL was permitted to adopt a differentiated regulatory framework based on bank asset size, scale, diversity, and complexity of operations in order to strengthen the supervision on systemically important banks while minimising regulatory compliance cost of small banks.

ix. Liquid Assets: The reference to liquidity requirement cited in the Act (Statutory Liquid Assets Ratio) has been discontinued as it is a backward-looking approach which does not reflect the true position of the liquidity of LCBs and Licensed Specialised Banks (LSBs). Instead an amendments was introduced requiring LBs to maintain liquid assets that are required to meet its liabilities as maybe determined by CBSL from time to time, and to comply with the requirements on liquidity having regard to the developments in the regulatory requirements and CBSL shall, as far as practicable, adopt international standards applicable on liquidity requirements, Further,

CBSL may determine additional liquid assets required to be maintained by LCBs and LSBs to meet liabilities from time to time and licensed banks are required to maintain such assets as determined by CBSL.

x. Capital: A new provision has been added for CBSL to require LCBs to maintain additional capital as appropriate considering the specific risks emanating from the business of such LCB.

xi. Restrictions on payment of dividends: In terms of the amendments, CBSL may issue Directions having considered the capital or liquidity levels of LCBs, providing conditions that need to be met by banks prior to payment of any dividends or transfer of profits earned in Sri Lanka, where appropriate.

xii. Accounts and Audit: Timeline for submission of financial statements by banks has been changed from 5 months to 3 months and the Auditor is required to submit the audit report within 2 months from the end of the financial year (previously 3 months). With respect to the external Auditor, a new provision has been included to replace the external Auditor of a bank once every 06 years and to replace the engagement partner once in 03 years. A transitional period of two years has been granted in this regard.

xiii. Large Exposures: With a view to minimising the credit concentration risk of LBs, provisions on large exposures¹ that can be granted by an LB commensurate with its capital has been broadened to include the concepts of “control

¹ any on balance sheet and off-balance sheet credit facility including but not limited to loans, overdrafts, advances or any commitment to grant loans, and all debt and equity investments, excluding equity investments in financial subsidiaries.

relationship” and “economic interdependence” in line with the international best practices. A transitional period of three years or another period as determined by CBSL has been granted for banks to comply.

xiv. Related Party Transactions: Considering the Basel Core Principles and international best practices, individuals and entities that can be considered as related parties of an LB have been expanded and a provision has been introduced to apply certain provisions relating to accommodation granted to directors and their close relations, to other related parties as well. Accordingly, the holding company of the bank, subsidiaries of that holding company, directors of those companies, directors of subsidiaries and associates of the bank and common directors are identified as related parties.

xv. Corporate Governance: In general, corporate governance determines the allocation of authority and responsibilities by which the business and affairs of a bank are carried out by its board and senior management. Best practices in corporate governance are vital to the effective functioning of the banking sector and the economy as a whole. Accordingly, strengthened requirements for qualifications, fit and proper assessments, and board responsibilities were introduced as amendments. The key amendments in BA pertaining to Corporate Governance are;

- provisions of the Banking Act on Corporate Governance to prevail over any other written law.
- provide information for fit and proper assessment before the appointment of a director.
- require having both academic/professional qualifications and (currently ‘or’) effective experience in banking, finance economics, accounting, business administration, information technology, risk management, law or any other relevant discipline as may be determined by CBSL, while the discipline category of ‘Administration’ has been removed as it a general category.
- require Director/CEO/KMP not be subject to any proceeding, inquiry or investigation (currently investigation or inquiry) consequent upon being served with notice of a charge involving fraud, deceit, dishonesty or other similar criminal activity by any court, tribunal, regulatory or supervisory authority, professional association, Commission of Inquiry, or other body established by law, in Sri Lanka or abroad.
- the right of the Director of Bank Supervision to conduct further investigations in relation to appointments and fit proper criteria, if necessary.
- the number of members of the Board of Directors of a licensed bank to be determined by CBSL and the minimum number will be specified as 7.
- CEOs and KMPs of a licensed bank shall be fit and proper persons for the respective positions as may be determined by CBSL in accordance with criteria set out in the Banking Act.
- CBSL to determine persons not fit and proper even after the cessation of the office as a Director/CEO/KMP, if they have committed or have been connected with the fraud, deceit, dishonesty or other similar

criminal activity or any other improper conduct, during the period in which he/she served in the respective position which may disqualify that persons to be a fit and proper person to be appointed, elected, or nominated as a Director/CEO/KMP.

- The provision on responsibilities of the Board of Directors of a licensed bank has been expanded specifying that the Board have the duty to oversee the management of the affairs of the licensed bank including its governance framework and is ultimately responsible for ensuring that the business of such bank is carried out in compliance with all applicable laws and consistent with safe and sound banking practices.

xvi. Offshore Banking: Considering the developments in the banking business locally and globally, the demarcation between the Offshore banking unit and the domestic banking unit of LBs has been eliminated. However, conducting offshore banking business has been added as a permissible activity of an LB in order to facilitate the existing OBU customers without impacting their businesses. In addition, an enabling provision has been included for CBSL to designate foreign currencies for the purpose of carrying on offshore banking business.

xvii. Vesting and Liquidation: With the enactment of the Banking (Special Provisions) Act No.17 of 2023, CBSL became the exclusive authority for resolution of LBs and provisions on measures that can be initiated by CBSL for resolution of LBs were included in the cited Act. Accordingly, certain provisions relating to vesting and compulsory liquidation of LBs were removed from the Banking Act, retaining provisions on voluntary liquidation.

xviii. Administrative Fines: Strengthening regulatory and supervisory powers, an enabling provision has been included for CBSL to charge administrative fines for certain areas such as liquidity, capital, large exposures, share ownership, and submission of financial statements. CBSL shall determine the procedure for imposing an administrative fine on a person and the amount of such fine, in proportion to the contravention so committed.

xix. Third-Party Information: CBSL may request to furnish information from third parties in order to discharge its powers, functions, and duties under the Banking Act.

xx. Approval and Concurrence of the Minister: Since the Minister has not been defined in the Banking Act, the Minister was defined as the Minister assigned with the subject of finance in terms of Article 44 or 45 of the Constitution. As per the new amendments the Minister's approval will be sought for the issuance of a new banking licence and other instances could be approved by CBSL. Accordingly Opening, closing, or relocating a branch or representative office outside Sri Lanka will be granted by CBSL in consultation with the Minister of Finance. In addition, in terms of the amendments, the following instances where the Banking Act requires the concurrence or approval of the Minister can now be approved by CBSL considering that there will be no direct fiscal implications.

- opening, closing, relocating a branch, agency or office in any part of Sri Lanka
- for a foreign bank to open a representative office in Sri Lanka

- acquisitions and mergers of banks
- acquiring material interest in a licensed commercial bank
- determining the amount of assigned capital to be remitted by the branch of a foreign bank intending to conduct banking business in Sri Lanka
- determining minimum capital requirements for licensed banks
- designating foreign currencies to conduct offshore banking activities

Conclusion

CBSL has issued necessary regulations to the banking sector to facilitate the effective implementation of the Banking (Amendment) Act

in the areas of corporate governance, related party transactions, offshore banking business, liquidity requirements, etc. With the implementation of the amendments to the Banking Act, it is expected that regulations and supervision over licensed banks will be further strengthened. In terms of the Banking Act and Banking Act Directions issued thereunder, the best practices in corporate governance of licensed banks will be established and persons with required qualifications and experience will be appointed as Directors/CEOs and KMPs of licensed banks. In addition, these amendments will facilitate smooth conduct of banking business and thereby ensure the resilience and stability of the banking sector in Sri Lanka.

(Source: Banking Act No.30 of 1988, as amended and Banking (Amendment) Act No.24 of 2024)

Central Bank Communication for Effective Monetary Policy Implementation

Udeshika Wijegunaratne

Senior Assistant Director
Communications Department

1. Introduction to Central Bank Communication

The dissemination of information by a central bank to its different types of stakeholders including the public on a range of economic and financial aspects such as monetary policy objectives, monetary policy implementation decisions, economic outlook, financial system related decisions, other policies and measures adopted by the central bank and future policy decisions, is known as central bank communication. Central banks communicate to enhance transparency, shape expectations, foster accountability, and advance their various objectives of preserving price stability, safeguarding the stability of the financial system and encouraging full employment.

The success of central banks is determined by their ability to assist citizens navigate the larger economic forces at play and understand how policies influence them, leading them to make better economic decisions. However, the performance of central banks is measured by results and economic

consequences. These initiatives strengthen public trust, enhance legitimacy, optimize and improve policy decisions. Insufficient communication from central banks can result in various negative consequences including, increased uncertainty, disturbances in the markets, loss of credibility, and decreased policy effectiveness, hence impeding the central bank's capacity to accomplish its goals and uphold financial stability. Therefore, in order for central banks to carry out their objectives and promote economic stability and prosperity, prompt, clear, and transparent communication is crucial. Effective communication can influence financial markets, improve monetary policy predictability, and support central banks' macroeconomic objectives. The wide range of communication strategies implemented across central banks around the world shows that an optimal communication strategy has yet to be determined.

This article explores the fundamentals of central bank communication, its guiding principles, and how various central banks implement their strategies globally. Core principles of Central

Bank Communication have been discussed as transparency, clarity, and timeliness, and their role in strengthening central banks’ credibility and effectiveness. An overview has been provided of how central banks communicate their monetary policy decisions and strategies, including historical shifts and current practices. Article has looked at how the Central Bank of Sri Lanka (CBSL) communicates its monetary policy in detailed, including specific practices and challenges. Comparative analysis of communication strategies employed by central banks around the world has been examined as a global perspective, highlighting best practices and innovative approaches.

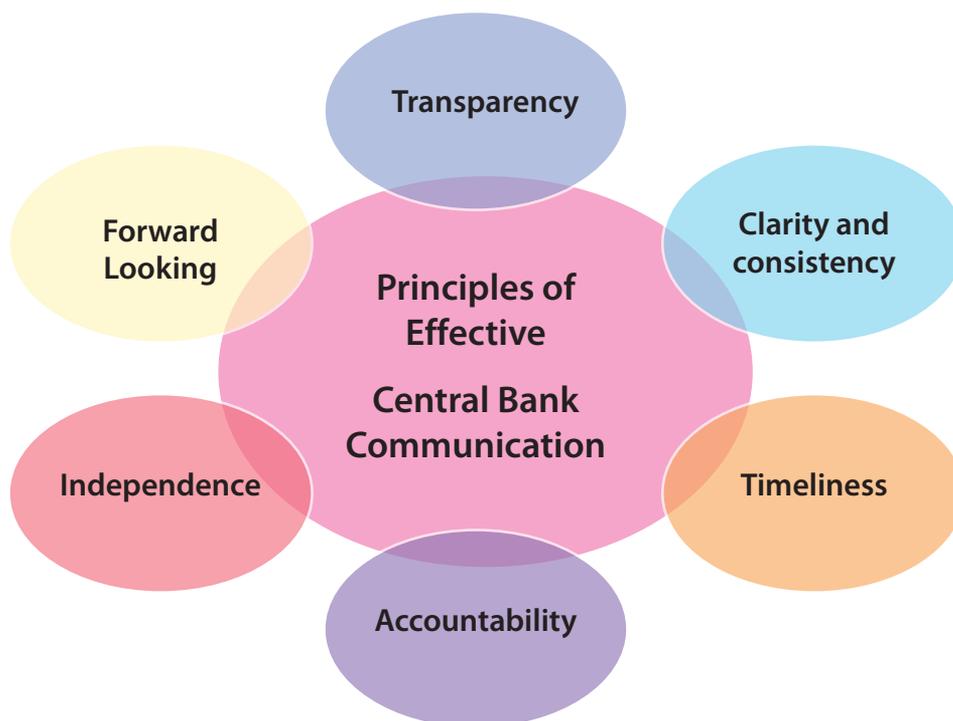
2. Principles of Central Bank Communication

Clear communication by central banks is widely acknowledged as crucial for increasing credibility, improving monetary policy effectiveness, and reinforcing accountability. This recognition has

been influenced by several factors over time. Firstly, the ability of communication to influence market expectations has been recognized by central banks progressively. Secondly, there has been an uptick in the need for comprehensive details regarding their objectives, decisions, and steps from both specialists and the general public. Third, communication enhances monetary policy efficacy and fosters public support for central bank independence, something that central bankers come to recognize and value. Improved and open communication is crucial for maintaining central banks’ independence and, eventually, their responsibility. Having considered this tendency, the principles of modern central bank communication can be depicted in figure 1 below.

2.1. Transparency: Transparency and active communication with different types of stakeholders of the central banks became

Figure 1: Principles of Central Bank Communication



Source: Author’s concept

2.3. Timeliness: The principle of providing information promptly and efficiently to the stakeholders, enabling them to have access to relevant information in a timely manner, to make informed decisions and react appropriately to changes in monetary policy and economic conditions.

2.4. Accountability: Central banks implement accountability mechanisms to guarantee that their policies are transparent, accountable, and open to review. Accountability is not achievable without transparency. In this regard, while making information easily accessible to the public through various communication channels, central banks explain the rationale behind their policy decisions, including their assessment of economic conditions, inflation outlooks, and risks to financial stability.

2.5. Independence: By emphasizing independence in communication, central banks maintain credibility, foster public trust, and promote economic stability by ensuring that policy decisions are made based on economic fundamentals rather than political expediency. This independence allows central banks to make decisions in the best interest of achieving their objectives, such as price stability, financial stability and full employment.

2.6. Forward looking: This highlights the significance of forecasting future economic situations and possible policy measures in advance. In order to manage public expectations and maintain market stability, it entails clear, proactive communications. This builds credibility and confidence in the central bank's dedication to economic stability. Informed decision-making and adjusting expectations are facilitated for different stakeholders.

3. Monetary Policy Communication

The strategies and channels used by central banks to inform the general public, financial markets, and other stakeholders about their monetary policy decisions, objectives, and outlook are referred to as monetary policy communication.

In a well-known blog post, former chairman of the Federal Reserve Ben Bernanke stated that monetary policy is 98 percent talk and 2 percent action. One of the Fed's strongest instruments was its capacity to influence market expectations of future policy through public statements. Bernanke's remark emphasizes that monetary policy actions frequently have an impact that is equal to or greater than the perception and anticipation of those actions. A central bank's capacity to influence expectations and communicate clearly is a powerful instrument to manage the state of the economy.

The communications strategies used by central banks have changed dramatically during the past decades. People started to realize how important it was to be transparent and to work with the markets rather than against them. Hence, communication strategy has proven to be a crucial tool for Central Banks, and this has become even more crucial since they started implementing inflation targeting frameworks (IT) as their monetary policy frameworks, under modern Central Banking arena. This sensible shift in communication was led by inflation-targeting central banks. In 1990, New Zealand was the pioneer in inflation targeting. In February 1991, Canada became the second nation to formally take on inflation targeting.

These inflation-targeting Central Banks determine their target interest rates in meetings to discuss monetary policy. As is the common practice around the world, press releases comprising of present

policies, the state of the economy, and indications of expected future policy, that provide an explanation of the policy's reasoning are then used to publicize these decisions. At least four different monetary policy-related aspects are discussed by central banks in their communications: the economy, monetary policy goals and strategy, the reasons behind specific policy choices, and their plans for future monetary policy direction.

Transparency and communication have become fundamental principles of central banks over time. Different kinds of transparency are explained in the literature on monetary policy transparency as operational, knowledge, and goal transparency. Operational transparency focuses on the clarity of the policy decision-making process and its implementation, while knowledge transparency emphasizes the data and analysis supporting policy decisions. Goal transparency ensures that the central bank's mission and policy objectives are clearly communicated. All of these aspects work together to promote predictability, accountability, and trust in monetary policy. By issuing thorough policy pronouncements and regular updates, central banks like the Federal Reserve and the European Central Bank have demonstrated their commitment to these principles. These practices have significantly increased market predictability and public understanding of monetary policy decisions.

The emergence of digital media has further advanced these principles and revolutionized central-bank communication. A wider audience may now be reached, and real-time information can be given by central banks more easily through platforms like social media, interactive websites, and livestreaming of press conferences. This change has improved accessibility and made it

possible to interact with stakeholders more directly. Central banks can access real-time feedback from financial markets and the general public through these means and make any required modifications. As a result, modern tools increase transparency's effectiveness and encourage closer engagement with stakeholders.

4. Monetary Policy Communication at CBSL

The Central Bank of Sri Lanka (CBSL) prioritizes transparency in its monetary policy operations. The Central Bank of Sri Lanka Act (CBA) No:16 of 2023 has authorized the Monetary Policy Board (MPB) of the CBSL to make decisions regarding monetary policy of the country and to implement a flexible exchange rate regime in line with the flexible inflation targeting framework.

To enhance transparency in its monetary policy actions, CBSL strives to remain in constant communication with market participants and the public. This approach supports accomplishing its primary objective of achieving and maintaining its domestic price stability. Monetary policy decision including adjustments to interest rates, along with their underlying rationale, provides comprehensive insights into current and anticipated macroeconomic conditions, inflation trends, and policy direction, enabling stakeholders to make informed decisions while supporting overall economic stability.

Section 26 of CBA denotes that, in order to specify the inflation target that the CBSL must meet, the Minister of Finance and the CBSL must sign a monetary policy framework agreement. As a result, the CBSL and the Minister have signed a Monetary Policy Framework Agreement [http://documents.gov.lk/files/egz/2023/10/2352-20_E.pdf], which outlines the inflation target that the CBSL must meet. In accordance with this Agreement, the CBSL

is supposed to achieve a quarterly headline inflation rate of 5% based on the Colombo Consumer Price Index.

The stance on monetary policy is typically reviewed by the MPB six times a year. At the beginning of each year, the dates of these six meetings are made public through the **monetary policy advance release calendar**, via corporate website of CBSL. Every time the MPB meets, the Monetary Policy Committee (MPC) chaired by the Governor and comprising of the directors of the related departments of CBSL including Economic Research, Domestic Operations, Statistics and International Operations, gives a thorough report on the state of the economy, as well as updates on the financial markets and the macroeconomy both domestically and internationally. Additionally, the MPB receives recommendations from the MPC about monetary policy from its technical studies and forecasts. The MPB makes appropriate monetary policy decisions that best meet existing and anticipated economic conditions, based on these technical analysis and recommendations. The Deputy Director of the Economic Research Department, overseeing Money and Banking division would serve as the Secretary to the MPC.

Figure 2 below depicts the monetary policy decision-making process of the CBSL, which explains the stakeholders and key functions, and how the decisions are eventually transmitted to the markets through effective communication.

In addition to announcing the inflation targets, CBSL works to uphold its trust with the public by promptly disseminating the monetary policy actions along with information regarding the state of the economy. The Communications Department of CBSL is responsible for disseminating monetary policy related information to its stakeholders.

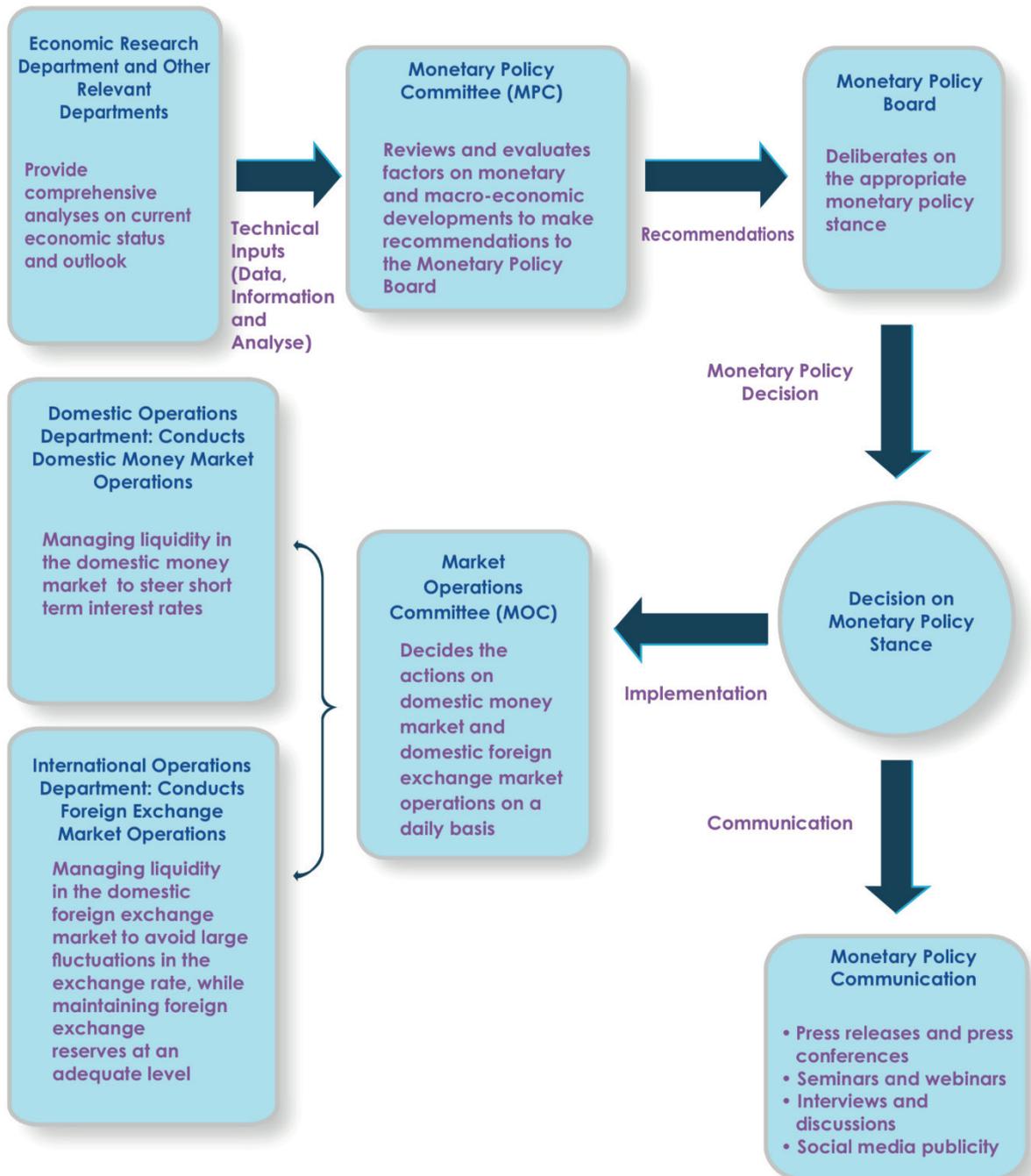
Six times a year, CBSL issues **press releases** announcing its decision on monetary policy stance, accompanied by an explanation of the factors influencing the decision and its rationale. CBSL ensures that all of its monetary policy communications follow the national language policy. Hence the press releases are published in all three languages. Being the focal communications platform of CBSL, the **corporate website** is regularly updated in all three languages to reflect any necessary changes to the monetary policy stance.

Having identified the importance for central banks to guide the perception and expectations of economic agents towards the desired path of inflation, the **inflation fan chart** is now a standard feature of the monetary policy communications of CBSL. While depicting the forecasting distribution of inflation based on the information available at a particular time, fan chart incorporated in the monetary policy press release, communicates the projected future path of the inflation, along with uncertainties of that projected path.

The CBSL publishes Monetary Policy Snapshots, titled **Monetary Policy Review at a Glance**, which are non-technical summaries of monetary policy press releases available in all three languages. These snapshots aim to enhance understanding of monetary policy decisions among diverse audiences by presenting technical information in a simplified manner, tailored to stakeholders with varying levels of expertise.

A report on monetary policy predictions made by other institutions as reported in the media is compiled by the Communications Department of the CBSL and distributed to the members of MPC and MPB.

Figure 2: Monetary Policy Decision-Making Process of the CBSL



Source: Monetary Policy Implementation in Sri Lanka, CBSL, July 2023

To equip management with valuable insights into potential media narratives and enable more effective messaging and proactive responses, the Communications Department will submit a **Media Predictability Report** to management ahead of each monetary policy press conference. This initiative aims to enhance preparedness for press

engagements, ensuring more comprehensive and satisfactory responses to media inquiries, thereby fostering public trust and reducing uncertainty.

The Monetary Policy Press Conference chaired by the Governor and senior Central Bank officials following each monetary policy review, is open

to the print and electronic media. In order to provide a wider audience with simultaneous access to the same material, proceedings are also **livestreamed on CBSL social media platforms**, particularly on Facebook, YouTube and LinkedIn platforms. During the press conference, the senior management address inquiries from journalists by opening the forum for two-way communication. Financial markets closely monitor these events for indications regarding forthcoming policy measures.

CBSL has gradually improved its **digital presence** for the monetary policy communications, through the **social media posts** on monetary policy stance on each of its social media channels, and through the use of **short video clippings** that feature the Governor and other senior officials of CBSL, explaining the monetary policy stance and current economic outlook, by capturing from the highlights of the press conference. Presentations made at each monetary policy press conference are available on YouTube for replay [in all three languages]. Engaging **explanations on the fan chart** are available on social media together with a picture and associated commentary. In order to raise understanding of monetary policy-related issues that arise with the different groups of its stakeholders, CBSL has updated its **frequently asked questions** and published structured answers to its corporate website. Moreover, senior central bank officials frequently engage in **media interviews** to share their perspectives on economic developments, policy priorities, and the outlook for monetary policy. These communications have the potential to impact public opinions of the CBSL's credibility and effectiveness, as well as market expectations.

Information concerning monetary policy operations and other pertinent economic data is also shared

through **daily/weekly/monthly indicators, monthly bulletins, periodicals, press releases, the key publications.**

At the end of each monetary policy cycle, a post-mortem analysis of **Monetary Policy Communication Effectiveness Reach** is carried out by the Communications Department to see how well the media personnel have interpreted the messages that the CBSL has been spreading during the monetary policy review and submit the findings to the management of the CBSL.

Statutory publications related to monetary policy include the Annual Economic Review (AER) and the biannual Monetary Policy Report. Starting in 2025, the Monetary Policy Report will be published quarterly following each major policy review. Additional publications include a pamphlet on Monetary Policy Implementation. While addressing monetary policy communication with the provisions of “Accountability”, the section 80 of the CBA specifies that, CBSL shall, once in every six months and at such additional times as it deems necessary, inform the public regarding the implementation of its monetary policy, and the achievement of its objects. This has more specifically been provisioned in section 27 of CBA. As a result, the CBSL issues a report biannually, namely, the “**Monetary Policy Report**” (MPR) detailing current inflation movements, inflation sources, medium-term inflation projections, and key risks to such projections, as well as monetary policy implementation. This explains to the public and other interested parties the rationale behind the monetary policy decisions made during the pertinent review period. It also offers guidance on the outlook for inflation and economic growth as well as an evaluation of the risks associated with it. The MPR issued by the CBSL will carry all macroeconomic projections. This has strengthened

MPR's position as the premier publication focused on macroeconomic outlook and policy in support of monetary policy objectives. In line with the CBSL's legislative accountability described by the CBA, the AER has been served as a key publication that communicates the state of the economy during a financial year emphasizing its policy objectives and the condition of the financial system. The report includes a review and an assessment of the policies of the Central Bank followed during such financial year. Concurrently, as has been the CBSL's practice since the pre-FIT policy framework, the dissemination of the MPR's key messages would be the primary emphasis of its outreach and communication campaigns following the implementation of the FIT policy framework, as opposed to the AER's.

Following the publication of the monetary policy report, **expert meeting on macroeconomic outlook** as interactive technical discussions is held as part of **awareness workshops** organized by CBSL, for media professionals, journalists, and other professionals including bankers, academics, private sector economists and experts in the financial sector.

The adoption of an inflation targeting framework and a greater emphasis on digital interaction while focusing on layered communication are two recent developments to the CBSL's monetary policy communication strategy. However, the bank faces ongoing challenges, such as ensuring effective multilingual communication, adapting to rapidly changing economic conditions, and balancing transparency with market sensitivity in its messaging. Addressing these challenges is crucial to maintaining the credibility and effectiveness of the CBSL's communication efforts.

With the intention of raising stakeholder awareness and information on monetary operations conducted

by the Central Bank in accordance with the current monetary policy stance, CBSL published its first **"Market Operations Report"** in July 2024. Enhancing the awareness and knowledge of the economy's stakeholders about the Central Bank's monetary policy and market operations is the purpose of this biannual report, which is produced as part of its overall communication strategy.

5. Monetary policy communication at different Central Banks around the world

The ways that various central banks across the world communicate their monetary policies varied owing to a wide range of factors, including institutional frameworks, cultural norms, and the degree of economic development. Monetary policy communication strategies implemented by several selected central banks in different regions can be summarized as follows.

5.1. Bank of Canada (BoC) - Canada:

The Bank of Canada (BoC) formulates monetary policy through its Governing Council, which meets eight times a year to set the target for the overnight rate, signaling its policy stance. At the core of Canada's monetary policy framework is a 2% inflation-control target within a 1–3% range, first established in 1991 and reviewed every five years, most recently renewed for 2022–2026. Communication is a vital component of the BoC's strategy, underpinned by an annual schedule of publications and events designed to keep stakeholders informed about evolving economic conditions and inflation trends. After each meeting, the BoC issues a press release on its website, followed by a press conference led by the Governor to explain decisions and respond to media inquiries. Quarterly Monetary Policy Reports provide detailed projections and risk assessments, while council members engage with the media to elaborate on decisions. Additionally, meeting

minutes, released two weeks after each session, offer further insights into the Governing Council's deliberations, reinforcing transparency, credibility, and the BoC's effectiveness in managing market expectations and maintaining economic stability.

5.2. Czech National Bank (CNB) – Czech Republic:

The Czech National Bank (CNB) formulates monetary policy through its Bank Board, which meets eight times a year to set the two-week repo rate, signaling its policy stance. As one of the leading central banks following global best practices in monetary policy communications for inflation targeting, the CNB targets 2% inflation and employs diverse tools to explain decisions and share economic insights. After each meeting, a press statement is promptly published on the CNB website, followed by an afternoon press conference led by the Governor and media interviews with board members to elaborate on policy rationale. Eight days later, the CNB releases non-technical meeting minutes alongside forward-looking inflation reports, which are also shared with experts during seminars and supplemented with explanatory media articles. Additionally, six years after each meeting, the CNB discloses situation reports and internal protocols, offering comprehensive transparency and reinforcing its credibility.

5.3. European Central Bank (ECB) - Eurozone:

The European Central Bank (ECB) emphasizes effective and transparent communication as critical to the success of its monetary policy. Every six weeks, the ECB's Governing Council meets to decide on steps to maintain its 2% inflation target, with decisions immediately explained in live-streamed press conferences led by the President and Vice-President. These events, accompanied by a Q&A session, provide insights into the Governing

Council's rationale and are detailed on the ECB's website, along with statements on interest rates, economic developments, and future outlooks for the euro area. Four weeks after each meeting, the ECB publishes meeting accounts summarizing discussions, financial and economic reviews, and policy considerations. To enhance accessibility, the ECB uses visual statements to simplify policy decisions and employs the ECB Blog and global presentations by Executive Board members to deepen public understanding of monetary policy and its implications.

5.4. Bank Negara Malaysia (BNM) – Malaysia:

BNM formulates monetary policy through its Monetary Policy Committee (MPC), which is responsible for policy development and operations, with the Overnight Policy Rate (OPR) as the primary signal of its stance. While BNM does not explicitly adopt an inflation targeting framework, the MPC meets six times annually, with agendas published online beforehand. Following each meeting, BNM issues a monetary policy statement summarizing decisions, occasionally supplemented by press conferences or media briefings. Regularly published quarterly reports and an Annual Report provide detailed analyses of monetary policy, inflation trends, and economic developments. BNM leverages its official website and social media channels to ensure stakeholders have timely and relevant information. BNM does not practice releasing the minutes of its MPC meetings.

5.5. Bank of Thailand (BoT) – Thailand:

The BoT aims to achieve medium-term price stability, sustainable economic growth, and financial stability through its monetary policy. Each December, the BoT and Thailand's Minister of Finance agree on the upcoming year's monetary policy goals, including medium- and long-term

inflation targets, which are then presented to the cabinet for approval. For 2024, the inflation target range is set at 1–3%. The BoT’s Monetary Policy Committee, which meets six times a year, formulates policy by setting the policy interest rate and determining the monetary stance. After each meeting, the BoT publishes a press release explaining its decisions and justifications, accompanied by a press conference led by the Governor. Quarterly Monetary Policy Reports provide detailed analyses of the economy, inflation forecasts, and factors influencing policy decisions. Meeting minutes, offering comprehensive insights into deliberations, are released two weeks after each session. To enhance public understanding, senior BoT officials deliver speeches and host seminars, supporting the bank’s goals of economic stability, transparency, and effective communication.

5.6. Bank of England (BoE) - United Kingdom:

The Bank of England (BoE) communicates its monetary policy decisions, aimed at maintaining a 2% inflation target, through its Monetary Policy Committee, which meets eight times a year. After each meeting, the BoE publishes a Monetary Policy Summary detailing key decision, the rationale behind them, and the voting outcomes, along with the meeting minutes that provide additional context and differing viewpoints. Dates for announcements, meeting minutes, and quarterly Monetary Policy Reports, which include economic analyses and inflation projections, are published annually on their website. Transcripts of MPC meetings are released with an eight-year lag. Following some meetings, the Governor conducts press conferences to explain decisions and address media and stakeholder inquiries, while senior officials engage in public appearances to further communicate the bank’s policy stance and economic outlook.

5.7. Federal Reserve System (FED) - United States:

The FED emphasizes systematic and well-understood monetary policy, aiming to clearly communicate its objectives to the public. Policy decisions are made by the Federal Open Market Committee (FOMC), which meets eight times a year or more if needed. Decisions are communicated through press releases, statements, and press conferences led by the Chair of the Federal Reserve Board. Meeting schedules, policy statements, and minutes are published online, with detailed meeting minutes released three weeks post-meeting and transcripts and materials made available after five years. Quarterly, the Federal Reserve Board submits the Monetary Policy Report to Congress, detailing policy actions, economic developments, and future prospects. Additionally, board members, including the Chair, and Federal Reserve Bank presidents testify before Congress and deliver presentations to share insights on economic trends and policy decisions.

5.8. Summary of Global Best Practices and Areas for Improvement

Globally, central banks employ various approaches to convey their monetary policies, which are shaped by their distinct institutional frameworks, cultural settings, and economic conditions. Systematic and transparent communication is a top priority for the FED in the United States. Press releases, press conferences, and comprehensive meeting minutes are made available to the public three weeks after the meeting and are fully released after five years. In a same vein, the Canada’s BoC uses proactive communication, releasing extensive Monetary Policy Reports and meeting minutes along with a yearly program of press briefings and publications. In order to make complicated choices

easier to understand, the ECB of Euro Zone prioritizes openness and clarity through frequent press conferences, online summaries, and visual announcements. In addition, the BoE of England prioritizes openness by making lengthy meeting minutes, policy summaries, and frequent public appearances by top officials available.

Similar procedures are used by other central banks, like the BoT and the CNB, who place a strong emphasis on open communication via frequent updates, press conferences, and thorough reports. Whereas the BoT releases full minutes and quarterly Monetary Policy Reports two weeks after each meeting, the CNB is renowned for its prompt delivery of inflation reports and non-technical minutes. The BNM does not publish meeting minutes, but it does regularly provide policy statements and quarterly reports to uphold transparency even in the absence of a defined inflation targeting framework. These different strategies highlight the central banks' dedication to openness and engagement with the public, having the goal of managing market expectations and maintaining economic stability.

Despite the advantages stated above, central banks still have room for development. Concerns over the complexity of economic jargon can be alleviated by making information more understandable for the general public by simplifying technical terminology used in communications. As evidenced by the ECB's procedures, maintaining uniform multilingual material in all official languages can improve accessibility for a range of audiences. Increasing transparency further could boost stakeholder understanding and confidence by releasing more thorough meeting minutes. These upgrades have the potential to strengthen central banks' relationships with the general public and

increase the effectiveness of their monetary policy communication and awareness campaigns. A summary and a comparison of the global practices with respect to monetary policy communication is given in the table below.

6. Conclusion

Central banks have evolved over the past few decades from just being transparent with the markets to actively and genuinely engaging with the public they serve. Central banks have begun engaging the public in a more direct and complementary manner. Despite notable variations, central banks around the world share a common goal of enhancing transparency, managing expectations, and promoting public understanding of monetary policy.

CBSL prioritizes transparency and stakeholder engagement in its monetary policy communication, guided by the CBSL Act No. 16 of 2023 and a flexible inflation targeting framework. With a quarterly inflation target of 5%, CBSL communicates policy decisions through press releases, detailed reports like the Monetary Policy Report and Annual Economic Review, and tools such as fan charts and non-technical snapshots in all three languages. Enhanced digital engagement and media interactions ensure timely information dissemination, while internal tools like the Media Predictability Report provides management with insights into potential media narratives, aiding in preparation for press conferences. Despite challenges like multilingual communication, CBSL remains committed to adapting its strategies and maintaining credibility through initiatives like the Market Operations Report

The future of monetary policy communication will be shaped by innovation, the development of technology, and a commitment to accountability,

Table 1: Comparison of global practices of monetary policy communication

	Monetary Policy Framework	Operating Target	Targeted Inflation	Policy Decisions announcement calendar publish in advance	Number of meetings per year	Frequency of MPR publication (per year)
Sri Lanka	Flexible Inflation Targeting	Average Weighted Call Money Rate	5%	Yes	6	2
Canada	Inflation Targeting	Overnight Rate	2% (with a control range of 1-3%)	Yes	8	4
Czech Republic	Inflation Targeting	Two-week Repo Rate	2% (with a tolerance band of $\pm 1\%$)	Yes	8	4
Euro Zone	Inflation Targeting	Main refinancing operations rate	2%	Yes	8	4
Malaysia	Combination of inflation targeting and other macroeconomic objectives	Overnight Policy Rate	No explicit target	Yes	6	No
Thailand	Inflation Targeting	1-day Bilateral Repo Rate	1-3%	Yes	6	4
United Kingdom	Inflation Targeting	Bank Rate	2%	Yes	8	4
United States America	Dual Mandate (Maximizing employment & Stabilizing prices)	Federal Funds Rate	2%	Yes	8	4

Source: Relevant Central Banks websites and IMF Technical Assistance Mission Report, May 2024

transparency, and engagement among stakeholders. Central banks will keep transforming their communication strategies to fulfill evolving stakeholder demands and expectations while successfully achieving their objectives. In global context, central banks are likely to increasingly utilize digital communication channels, such as social media, interactive websites, and mobile applications to facilitate real-time dissemination of information and foster greater transparency and accessibility. Artificial intelligence technologies will also come into play in terms of forecasting and scenario analysis, enhancing the effectiveness of forward guidance and policy communication.

In order to improve their monetary policy communication strategies and provide stakeholders

with personalized and data-driven insights, central banks will be expected to use advanced technologies like artificial intelligence and machine learning more and more in the future. In addition, the incorporation of sophisticated digital platforms and interactive tools would enable instantaneous interaction and feedback, enabling central banks to react more efficiently to public concerns and market conditions, ultimately boosting transparency and confidence in general.

References:

1. *Bank of England* (2024). Available at: <https://www.bankofengland.co.uk/> (Accessed: 21 March 2024).
2. *Bank of Thailand* (2024). Available at: <https://www.bot.or.th/en/home.html> (Accessed: 28 July 2024).

3. *Bank Negara Malaysia* (2024). Available at: <https://www.bnm.gov.my/> (Accessed: 21 March 2024).
4. Blinder, A.S. *et al.* (2008) ‘Central Bank Communication and Monetary Policy: A Survey of Theory and Evidence’, *Journal of Economic Literature*, 46(4), pp. 910–945. doi: <http://www.jstor.org/stable/27647085>
5. Blinder, A.S. *et al.* (2022) *Working Paper Series No 2694: Central Bank communication with the general public: promise or false hope?*, Available at: <https://www.ecb.europa.eu/pub/pdf/scpwps/ecb.wp2694~a5e2951c42.en.pdf> (Accessed: 19 March 2024).
6. Bulir, A, & Smidkova, K. (2008) ‘Striving to be “clearly open” and “crystal clear”: Monetary policy communication of the CNB’, IMF Working Paper No. 2008/84. Washington, D.C.: International Monetary Fund. Available at: <https://www.imf.org/en/Publications/WP/Issues/2016/12/31/Striving-to-Be-Clearly-Open-and-Crystal-Clear-Monetary-Policy-Communication-of-the-CNB-21853> (Accessed: 01 July 2024).
7. Bundick, B, & Smith, A.L. (2018) ‘Did communicating a numerical inflation target anchor U.S. inflation expectations?’ FOMC Secretariat. Available at: <https://www.federalreserve.gov/monetarypolicy/files/FOMC20180117memo01.pdf> (Accessed: 03 August 2024).
8. Central Bank of Sri Lanka (2023) *Monetary Policy Implementation in Sri Lanka*. Available at: https://www.cbsl.gov.lk/sites/default/files/cbslweb_documents/publications/DOD_pamphlet_monetary_policy_implementation_in_sri_lanka_e.pdf (Accessed: 19 March 2024).
9. Central Bank of Sri Lanka (2024) *Monetary Policy Report*. Available at: <https://www.cbsl.gov.lk/en/publications/economic-and-financial-reports/monetary-policy-reports/monetary-policy-report-2024-february> (Accessed: 19 March 2024).
10. Communication: A vital tool in the implementation of monetary policy, Remarks by Paul Jenkins Senior Deputy Governor Bank of Canada to the FMAC/FMA-USA joint conference 2004 Toronto, Ontario 30 September 2004, Available at: https://www.bankofcanada.ca/wp-content/uploads/2010/06/jenkins_e.pdf (Accessed: 03 August 2024).
11. *Czech National Bank* (2024). Available at: <https://www.cnb.cz/en/> (Accessed: 30 June 2024).
12. Ehrmann, M, & Fratzscher, M. (2005), *How Should Central Banks Communicate?* Available at: <https://www.ecb.europa.eu/pub/pdf/scpwps/ecbwp557.pdf>
13. Eijffinger, S.C.W, & Petra, M.G. (2006) ‘How Transparent Are Central Banks?’, *European Journal of Political Economy*, 22(1), pp. 1-21. doi: <https://doi.org/10.1016/j.ejpoleco.2005.09.013>
14. European Central Bank (2024). Available at: <https://www.ecb.europa.eu/ecb/html/index.en.html> (Accessed: 21 March 2024).
15. Fay, R, & Hess, K. (2016) ‘Monetary policy frameworks: Recent international developments’, *International Economic Analysis Department, Bank of Canada Review*. Available at: <https://www.bankofcanada.ca/wp-content/uploads/2016/05/boc-review-spring16-fay.pdf> (Accessed: 03 August 2024).
16. Federal Reserve System (2024). Available at: <https://www.federalreserve.gov/> (Accessed: 21 March 2024).
17. Government of Sri Lanka, “Central Bank of Sri Lanka Act, No.16 of 2023”, Government Printers.
18. Heenan, G, Peter, M, & Roger, S. (2006) ‘Implementing inflation targeting: Institutional arrangements, target design, and communications’, IMF Working Paper No. 2006/278. Washington, D.C.: International Monetary Fund. Available at: <https://www.imf.org/en/Publications/WP/Issues/2016/12/31/Implementing-Inflation-Targeting-Institutional-Arrangements-Target-Design-and-Communications-20089> (Accessed: 01 July 2024).
19. Jegajeevan, S. (2023), ABCs of the Inflation Fan Chart. Available at: https://www.cbsl.gov.lk/sites/default/files/cbslweb_documents/statistics/otherpub/information_series_note_20240206_abc_of_inflation_fan_chart.pdf (Accessed: 20 March 2024).
20. Liu, J. *et al.* (2022) ‘Can central bank communication effectively guide the monetary policy expectation of the public?’, *China Economic Review*, 75(2022), pp. 1–26. doi: <https://doi.org/10.1016/j.chieco.2022.101833>
21. Petrus, M, Remo, A, & Tonner, J. (May 2024), Technical Aide-Memoire, Sri Lanka, IMF Technical Assistance Mission on Developing a Forecasting and Policy Analysis System (FPAS) at the Central Bank of Sri Lanka, Institute for Capacity Development, International Monetary Fund.