Committed to professional excellence

बैंक क्वेस्ट

Bank Quest

(ISSN 00194921)

The Journal of Indian Institute of Banking & Finance (ISO 21001:2018 Certified) खंड / Vol 96 / अंक / No 01 - जनवरी - मार्च 2025 January - March 2025

CYBER RISK MANAGEMENT

IIBF - PUBLICATION LIST

Sr. No	Examination	Medium	Name of the Book	Edition	Published by	Price (Rs.)
1	CAIIB	English	Advanced Bank management	2023	M/s Macmillan Education India Pvt. Ltd.	930/-
2	CAIIB	English	Advanced Business & Financial Management	2023	M/s Macmillan Education India Pvt. Ltd.	810/-
3	CAIIB	English	Banking Regulations & Business Laws	2023	M/s Macmillan Education India Pvt. Ltd.	860/-
4	CAIIB	English	Bank Financial Management	2023	M/s Macmillan Education India Pvt. Ltd.	1005/-
5	CAIIB-Elective	English	Information Technology and digital banking	2023	M/s Macmillan Education India Pvt. Ltd.	640/-
6	CAIIB-Elective	English	Rural Banking	2023	M/s Macmillan Education India Pvt. Ltd.	830/-
7	CAIIB-Elective	English	Central Banking	2023	M/s Macmillan Education India Pvt. Ltd.	720/-
8	CAIIB-Elective	English	Human Resource Management	2023	M/s Macmillan Education India Pvt. Ltd.	975/-
9	CAIIB-Elective	English	Risk Management	2023	M/s Macmillan Education India Pvt. Ltd.	1390/-
10	JAIIB	English	Indian Economy and Financial System	2023	M/s Macmillan Education India Pvt. Ltd.	865/-
11	JAIIB	English	Principles and Practices of Banking	2023	M/s Macmillan Education India Pvt. Ltd.	1250/-
12	JAIIB	English	Accounting & Financial Management for Bankers	2023	M/s Macmillan Education India Pvt. Ltd.	825/-
13	JAIIB	English	Retail Banking & wealth management	2023	M/s Macmillan Education India Pvt. Ltd.	840/-
14	JAIIB	Hindi	Indian Economy and Financial System	2024	M/s Macmillan Education India Pvt. Ltd.	1700/-
15	JAIIB	Hindi	Principles and Practices of Banking	2024	M/s Macmillan Education India Pvt. Ltd.	2500/-
16	JAIIB	Hindi	Accounting & Financial Management for Bankers	2024	M/s Macmillan Education India Pvt. Ltd.	1700/-
17	JAIIB	Hindi	Retail Banking & wealth management	2024	M/s Macmillan Education India Pvt. Ltd.	1700/-
18	Certificate Course	English	Anti - money laundering and KYC	2023	M/s Macmillan Education India Pvt. Ltd.	445/-
19	Certificate Course	English	Treasury Management	2023	M/s Macmillan Education India Pvt. Ltd.	860/-
20	Diploma in Banking Technology	English	Design Development and Importance of Information System	2017	M/s Macmillan Education India Pvt. Ltd.	338/-

Contd. on Page No. 63

CONTENTS

Content Page

Special Features

Bank Quest

Volume 96, Number : 1

January-March 2025
(ISSN 00194921)

The views expressed in the articles and other features are the personal opinions of the authors. The Institute does not accept any responsibility for them.

लेखों तथा अन्य रचनाओं में व्यक्त किए गए विचार लेखकों के निजी विचार हैं । लेखकों द्वारा व्यक्त किए गए विचारों के लिए संस्थान किसी प्रकार से उत्तरदायी नहीं होगा ।

INDIAN INSTITUTE OF BANKING & FINANCE
Kohinoor City, Commercial-II, Tower-I, 2nd Floor, Kirol Road, Kurla (W), Mumbai - 400 070.
E-mail : admin@iibf.org.in
Website : www.iibf.org.in

MISSION

The mission of the Institute is to develop professionally qualified and competent bankers and finance professionals primarily through a process of education, training, examination, consultancy / counselling and continuing professional development programs.

ध्येय

संस्थान का ध्येय मूलत: शिक्षण, प्रशिक्षण, परीक्षा, परामर्शिता और निरंतर विशेषज्ञता को बढ़ाने वाले कार्यक्रमों के द्वारा सुयोग्य और सक्षम बैंकरों तथा वित्त विशेषज्ञों को विकसित करना है ।

Printed by Mr. Biswa Ketan Das, **published by** Mr. Biswa Ketan Das on behalf of Indian Institute of Banking & Finance and **printed at** Onlooker Press 16, Sasoon Dock, Colaba, Mumbai-400 005 and **published from** Indian Institute of Banking & Finance, Kohinoor City, Commercial-II, Tower-I, 2nd Floor, Kirol Road, Kurla (W), Mumbai - 400 070. **Editor** Mr. Biswa Ketan Das.

Editorial

Mr. Biswa Ketan Das
Chief Executive Officer,
IIBF, Mumbai

The ever evolving and dynamic nature of financial sector underscores the need of staying updated with the emerging trends, opportunities and challenges in the sector. As a part of Member Education series, the Institute annually organises Memorial Lectures on contemporary topics. In this issue of Bank Quest, we are publishing the transcripts of Memorial Lectures, Conference report and other contemporary articles.

The Institute had organised 14th Shri. R. K. Talwar Memorial Lecture on 27th February, 2025. The lecture was delivered by Shri. M. Nagaraju, Secretary, Department of Financial Services, Ministry of Finance on "Banking System for Viksit Bharat: Challenges and Opportunities". The speaker highlighted the key challenges such as ensuring universal financial inclusion, universal credit coverage and risks associated with advancing digital capabilities. The lecture received high acclaim from senior banking professionals for its depth and relevance. We are publishing the 14th Shri. R. K. Talwar Memorial Lecture as the first article of this issue.

The efficient risk management primarily includes better expression of risks, prioritisation across risk types and importantly, better recognition of risks. Aligned with this perspective, the second article is the lecture 39th Sir Purshotamdas Thakurdas Memorial Lecture delivered by Dr. Rabi Narayan Mishra on "From Fixing points of Instability to setting a state of Resilience making financial entities Distress-immune and Future-ready" on 14th November, 2024. The speaker discussed different forms of risks and advised bankers to act prudently. The lecture holds immense knowledge for the professionals working in banking and financial sector.

The financial sector is globally interconnected with risks and opportunities that are shared across borders. Recognizing the importance of discussion and collective efforts on International level, the Institute had organised 21st APABI International Conference on 13th-14th November, 2024 on the theme "Paradigm Shift in Banking-Moving towards a Resilient, Inclusive and Sustainable Model". The Conference consisted of Keynote addresses by Guest Speakers and four panel discussions on the topics of global importance. This issue features the 'Report of 21st APABI International Conference' focussing on the readers about the current trends and developments in the financial sector.

As the technology landscape in the financial sector is evolving rapidly, the associated risks are mounting. Cyber risk is one of such risks, which may have severe implications, if left unattended. Moreover, financial institutions remain prime target for cyber threats. Considering the necessity of prevention

and mitigation of cyber risks, we are bringing out this issue of Bank Quest on the theme "Cyber Risk Management".

The next article of this issue is jointly written by Dr. Sachin Sharma, Chief Manager (Systems), State Bank of India and Mr. Mukesh Ahuja, Assistant General Manager (Systems), State Bank of India on "Mitigating Cyber Threats in the BFSI sector: AI-driven Risk management and resilience strategies in Financial Intermediation". The authors have discussed the integration of emerging technologies such as Artificial Intelligence and Machine Learning with traditional risk management approaches in financial sector for enhanced efficiency.

The major hurdle in implementing the potential solutions is skill gap, especially, in implementing new technologies. Emphasizing the need of train the existing and potential professionals along with 360 degree approach encompassing Prevention, Detection, Response and Recovery to manage the cyber risks. Our next article is penned by Mr. Tushar Ranjan Barik, Assistant Professor, Kalinga University and Dr. Chandra Bhooshan Singh, Assistant Professor, Kalinga University on "360-degree approach to Cyber risk management as a strategic tool for fraud detection and prevention in banking".

The next article of this issue is on ''बचत और निवेश: बढ़ती संभावनाएं'' written by Mr. Sanjay Madhukar Nafde, Former Chief Manager, State Bank of India.

Though reading books, magazines and journals is a valuable source of knowledge, personal experience remains unparalleled. In this regard, we are publishing 'Book Review' of the Book, ''Banking beyond Borders'' written by Mr. Mohan Vasant Tanksale, Former Chairman, Central Bank of India and Executive Director, Punjab National Bank and reviewed by Dr. Brinda Jagirdar, Former Chief Economist, State Bank of India. The book offers a compelling narrative, capturing the rich experiences of a seasoned banker.

We hope this issue will be appreciated by its readers for its contents and coverage. We also encourage the bankers and academicians to contribute the articles in Bank Quest.

Suggestions and feedback for further improving the contents are welcome.

Biswa Ketan Das

BANKING SYSTEM FOR VIKSIT BHARAT: CHALLENGES AND OPPORTUNITIES

M. Nagaraju*

It is my privilege to deliver the fourteenth R. K. Talwar memorial lecture honouring the great legacy of late Shri Raj Kumar Talwar ji. He was truly an extraordinary leader of the banking industry, respected for his integrity, vision and service. His contribution to the banking industry and his accomplishments go far beyond his life of honesty, truthfulness and courage.

Fast forward to the current times, where developments across economies are happening at breakneck speed. As India has embarked on an ambitious journey of 'Viksit Bharat', it is pertinent to talk about the visions of Viksit Bharat and the onus of the same lying with our financial sector, led by banking, in augmenting India's fortune, in creating a strong economic entity promoting sustainable and inclusive growth amidst a disintegrated global landscape.

In this journey, I invite you all to time travel with me to experience the virtual reality of a robust and inclusive Viksit Bharat. While analysing the endeavours of our banking sector, I will also like to focus on the role of regulations, enabling a responsible yet frictionless pace of progress towards this ambitious mission.

Global Macro perspectives

The global economy is on a roller coaster ride. According to the International Monetary Fund (IMF)'s World Economic Outlook, January 2025, global growth is projected to be 3.3% for both 2025 and 2026, which is below the historical average of 3.7% during the last twenty years. While the United States (US) economy continues to show strength, the Eurozone is grappling with stagnation. Though inflation is expected to moderate, uncertainties and risks, including those arising from geopolitical tensions, trade protectionism, inward looking strategies and policy ambiguities continue to loom large.

The challenging global economic landscape is further complicated by the strong dollar, which strains emerging market currencies and heightens financial market volatility.

Strong Macro-economic dynamics: India's time

Prolonged geopolitical conflicts, geo-economic fragmentations, inward looking policies, renewed trade protectionism, competitive retaliation and emergence of trade war have created plenty of uncertainties in the global policy arena. India's growth, though not fully insulated from these vagaries, is driven by strong domestic fundamentals and much needed reforms.

Indian economy, ranked as 10th largest economy in the world in 2014, has risen to become the world's fifth-largest economy by nominal Gross Domestic Product (GDP) and the third largest in terms of purchasing power parity today. Indian economy maintains its stature as the world's fastest growing major economy in 2024 and is expected to upgrade its position in coming years. The well-coordinated fiscal and monetary policy in combination with structural reform have enabled building business friendly climate and has become home to the numerous global innovative firms.

Thanks to a confluence of factors, including the steps taken by the Government, the Indian economy has emerged as bright spot of stability and opportunity. We have not only kept our house in order against large

*Secretary, Department of Financial Services, Ministry of Finance.
14th Shri R. K. Talwar Memorial Lecture was delivered by Mr. M. Nagaraju, Secretary, Department of Financial Services, Ministry of Finance, on February 27, 2025, in Mumbai.

and overlapping global shocks but also improved our macroeconomic fundamentals and safety buffers. The balance sheets of banks and corporates are the healthiest in a long time and with the public investment push by the Government, have created favourable conditions in form of prime pumping for a sustained revival in investment.

Consumer confidence, which showed some signs of moderation in last couple of quarters, will certainly revive by the demand augmenting measures announced by the Honourable Finance Minister in the Budget 2025-26. As evident from surveys, revival in consumer demand, both in rural and urban areas is on a rising trajectory. Our external sector inspires confidence as we are reaping export opportunities in the services sector; our current account deficit remains eminently manageable; and we have bolstered our forex reserves with a 10+ months of import cover to deal with any potential adverse eventualities.

The large domestic consumption base of India constituting nearly 60-65% of GDP, helps India to insulate itself from the vagaries of global slowdown. With India's 1.43 billion populace with a median age of 28.2 years, 68% of the population belonging to the working age group. This helps the nation to enjoy demographic dividend and India is well poised to take advantage of this. Today, India has become the new global growth engine with its young demography, improving physical and digital infrastructure and above all, an enabling policy environment.

Viksit Bharat mission

Viksit Bharat 2047 is the vision to transform India into a developed nation by 2047, the centenary of India's independence. This vision encompasses developments across various segments of Indian Economy so that they rise from the current state to drive the agenda set by the Honourable Prime Minister's vision.

Our aspirations of Viksit Bharat 2047 aim to strive for: India's GDP to be USD 30 trillion from current ~USD 3.89 trillion; per capita income USD 18,000-20,000 from current ~USD 2,700; bank credit to private non-financial sector as % to GDP to be 130% from current 56%; achieving 100% financial literacy and many more.

Current challenges to Banking sector in its Viksit Bharat mission

Given the importance of banking system in supporting economic growth, the constraints the sector faces need to be addressed well in time so that the banking sector accelerates the wheels of Viksit Bharat mission. The first and foremost constraint of Indian banks is of having a strong capital base to support the Viksit Bharat mission and for which our banks would need to raise a significant amount of capital to support the country's economic growth. Hence, access to capital from international sources needs to be looked at and to be worked upon.

Ensuring universal financial inclusion is another major challenge. Banks need to create opportunities for every individual to grow and contribute to the nation's progress. This involves innovating and reimagining banking strategies to align with the evolving needs and preferences of customers. India needs to achieve 100% financial inclusion from current level of 64%. We need to work on developing more simplified micro-investment products. Financial awareness regarding financial products, digital transactions and other Government schemes in rural and remote areas needs to be accelerated. Also, the existing gender gap not just with respect to deposit account ownership but also with regards to access to credit needs to be overcome.

Expanding social security net is important through universal insurance and pension coverage. India's share in global premium is ~2%; Protection Gap in India is 87%. Given very low insurance penetration of 3.7% in FY23-24 in India against global average of 7%, banks need to support the masses to access the social security net, for the masses by financial literacy and product customization.

Large banks provide financing for large-scale projects, supporting massive infrastructure development requirement, driving economic growth

and development. Large banks play a crucial role in the stability and growth of the global economy as they have resources and expertise to absorb shocks and manage risks better, ensuring stability in the financial system.

From innovation angle, large banks are always preferred as large banks invest in financial technologies, promoting innovation in the banking sector, which lead to more efficient and accessible financial services. Moreover, large banks ensures that both businesses and individuals have access to reliable and efficient financial services as intermediation costs for banks decline and makes them efficient.

Apart from the above, universal credit coverage for Micro, Small and Medium Enterprises (MSMEs) and Agriculture is must. Given, the MSME sector contributes 30% India's GDP, 45% to exports and 62% to employment, we need to have robust credit flow to the agriculture sector and enabling the access to credit for the MSME sector and supporting entrepreneurship and generation of employment.

Advancing digital capabilities and future competencies is essential. The banking sector needs to harness the full potential of its workforce using digitization and emerging technologies like Generative Artificial Intelligence (GenAI).

Moreover, building a strong banking system that enhances global confidence in India's economy is important. This will attract more foreign investment and support the country's economic ambitions.

Our aspirations of Viksit Bharat need a strong base to be laid down by the current incumbents and leaders and subsequently to be driven by coming generations. Having said that, we need to introspect our current strength that can be leveraged and the emerging challenges that need to be addressed. The aspirations require systematic changes, institutional reforms and regulatory overhauling.

Banking in Viksit Bharat – Opportunities and Way forward

Viksit Bharat mission reckons banks to deliver on certain structural themes. To begin with, mobilising deposits on permanent basis may be a top priority. This is because households are turning net borrowers from the banking industry, aggravating pressure on margins and liquidity. Enhancing productivity is also important as it is seen that over the past decade, costs have risen faster than income. Productivity gains have lagged cost increases. As technology and compliance costs are expected to be higher in coming days, banks need to deploy innovative solutions to boost income. Building future ready capacity by fully embracing future capabilities such as operation and tech resilience, Environmental, Social and Governance (ESG), AI & GenAI is vital.

We need multiple globally competitive large banks having presence across the globe, facilitating access to global funds, best talent and technical expertise. Currently, only two Indian banks i.e. State Bank of India (SBI) and HDFC Bank feature in the Top 100 global banks by total assets, which is not strong enough in comparison to banks from China and the US, which dominate the top 10 global banks list.

The current banking conglomerates need to expand horizon, extend operations into global financial hubs, identify and acquire mid-sized global banks, utilize green bonds, sustainability-linked loans and foreign debt markets to fund domestic credit expansion. The size and scale would enable these transformed global banks to fund ultra large projects spanning across Infrastructure and Manufacturing, entailing setting-up peripheral industries and projects, thereby, catalysing job creation and urbanization.

MSME is another segment, which despite the best efforts of all stakeholders, continue to rely on funds outside the formal banking channels. Multiple institutional reforms have been undertaken during the last few years including the Union Budget 2025-26, that increased investment and turnover limits of MSMEs, expanded credit guarantees facility, schemes for dedicated support for first-time entrepreneurs etc. This may minimize the formal credit gap to the sector. Lending institutions need to leverage Digital Public Infrastructure (DPI), Unified Lending Interface

to expedite assessment and disbursement. However, the most important step is to handhold and support the MSMEs, which entails setting-up comprehensive support ecosystem that includes mentorship, financial literacy programs and advisory services to empower them in managing finances and making informed decisions. The new credit assessment method wherein the public sector banks have developed inhouse technology enables capabilities to assess MSMEs using their digital footprints instead of external assessments, aims to provide a more accurate evaluation and improve MSMEs' access to credit.

The National Infrastructure Pipeline (NIP) proposes an estimated expenditure of Rs.165 lakh crore over the next 5 years. With an envisaged Debt : Equity funding of 70:30, the NIP would require ~Rs.120 lakh crore of debt. The niche sectors like semiconductor require huge funding to set-up whole ecosystem. Financial sector needs to play the major role to make NIP a reality and provide funds towards capital intensive sectors.

While financing of capex and projects is vital, it is equally important that small ticket loans for employment generation grow even faster. Furthering of financial inclusion and unlocking productive potential of citizens is a national priority and a moral imperative. Schemes such as the Pradhan Mantri Jan Dhan Yojana (PMJDY), Pradhan Mantri Suraksha Bima Yojana (PMSBY), Pradhan Mantri Jeevan Jyoti Bima Yojana (PMJJBY), PM-SVANidhi, PM Vishwakarma, Micro Units Development & Refinance Agency (PM-MUDRA) Yojana etc. have contributed significantly in deepening financial inclusion in the country.

Digital payment system and FinTechs will play vital role in transforming the current state of economy. Digital transactions in India have grown over 90-fold during FY2013-24, constitute 99.5% of total payments in FY24. On the other hand, India is the third largest FinTech sector in the world with more than 13,000 fintech companies and a cumulative investment of more than USD 33 billion. These are testaments of the India's growing digital prowess and conducive policies and infrastructure in place. However, the future steps and initiatives would be more crucial than ever. We need to build a resilient policy and regulatory framework for fintech, putting in place- information repository, regulatory framework for FinTech, Digital Payments Intelligence platform to mitigate digital payment related frauds.

While strategic collaboration between banks and FinTechs have led to several innovations in the sector ranging from better customer service to last mile credit delivery, it calls for adequate safeguard to protect the digital infrastructure of institutions and customer endpoints.

Banks are expanding the skill development centres (Rural Self Employment Training Institutes or RSETIs) for handholding and providing technical training, setting up more Self-Help Groups (SHGs) across the country, imparting financial education and disseminating initial credit. Other stakeholders also need to pitch in to utilise their Corporate Social Responsibility (CSR) funds to provide all the basic support to these vulnerable segments, to uplift them from their current standing so that they become part of mainstream economy and actively contribute to the development.

The relentless reform and substantial investment in banks over the last few years has brought the banks to a position of strength, whereby, they have a strong capital base providing them enviable loss absorbing buffers. Credit growth is broad-based and is in double digit for last two years. To meet the growing credit demand, banks are raising capital from alternate avenues including capital market, long term bond, Certificate of Deposit (CD) issuances as well as through competitive deposit rates and drawing down their high-quality liquidity assets (excess Statutory Liquidity Ratio (SLR) deposits). Delinquency is at historic low level which is reflected through increased investor appetite for banking stocks, thereby, offering a good opportunity to reward shareholders and employees.

Today, the Indian banking system continues to be resilient, backed by improved asset quality, stable and broad-based credit growth and robust earnings growth. The reach and depth of financial intermediation is being aided by technology and growing digitalisation, which provide new opportunities for growth and financial inclusion. Tech innovations in the financial sector have improved

credit delivery mechanisms, improving the scope for further innovation in banking and financial products, and for furthering differentiated banking needs. The recent measures undertaken by the Government on digitalisation of the economy and availability of data provide a more objective and comprehensive basis for credit assessment and thereby, enhanced lending to both individuals and businesses.

The evolving Indian financial landscape is increasingly becoming innovation and tech-driven, with India Stack, Artificial Intelligence (AI), embedded finance and robotics playing an instrumental role in its transformation. New technologies like generative AI, quantum computing, digital infrastructure of institutions comes with both risks and benefits which need to be harnessed in a calibrated manner. Setting up sponsored research chairs/incubation centres in the institutes of eminence to carry out cutting-edge research will need to fast pace so that the future technology architectures are aligned with the visions of Viksit Bharat.

Our financial system is one of the forerunners in addressing the issue of 'last-mile connectivity' by leveraging its world-class digital public infrastructure which includes the Jan Dhan, Aadhar and Mobile (JAM) trinity; the Unified Payments Interface (UPI); the Open Network for Digital Commerce (ONDC); and the Account Aggregators (AAs) framework, differentiated banking/insurance licences, Central Bank Digital Currency (CBDC), the Open Credit Enablement Network (OCEN), Digilocker etc. continue to drive the digital march.

Government in close co-ordination with various stakeholders has taken a number of critical steps to ensure robust cyber security systems by banks through its regular IT examinations, assessing bank's compliance with cyber security regulations and guidelines, and identifying and addressing any vulnerabilities in their systems. However, the financial institutions, particularly banks, need to move a notch up now and should include stress testing of 'cyber risk' as part of their Risk Assessment to gauge the impact, in case of any cyber-attack on their systems. Regulators in Europe and Singapore have already initiated steps in this direction and banks in India too need to take appropriate steps.

While addressing growth, it is important to ensure that the growth is sustainable which asks for special focus on climate related concerns. India has been vulnerable, in varying degrees, to a large number of natural, as well as human-made disasters on account of its unique geo-climatic and socio-economic conditions. It is highly vulnerable to floods, droughts, cyclones, earthquakes, landslides, avalanches and forest fires.

More so, India's economy is highly dependent on nature as one third of its GDP comes from sectors greatly reliant on nature. The impact of devastating nature catastrophes various part of the country lately, have severely impacted the natural course of life and economy. Future climate change may be more brutal and therefore, calls for necessary actions.

The financial sector has an important role to play in the fight against climate change by supporting reductions in climate change risk and mitigating the impact of adverse climate events. Risks can be mitigated and minimized through the use of Green Financing, with objective of actively addressing climate change, reducing environmental footprint and promoting sustainability, which encompasses various financial instruments and mechanisms designed to channel capital toward environmentally responsible and sustainable projects and initiatives.

Our banking regulator, the Reserve Bank of India has joined the Central Banks and Supervisors Network for Greening the Financial System (NGFS) in 2021 and is expected to implement global best practices and contribute to the development of environment and climate risk management in the financial sector, while mobilising mainstream finance to support the transition towards a sustainable economy.

To sum up, Indian banking is well paced to support and accelerate economic growth for a Viksit Bharat. As reform is an ongoing effort, the regulator and Government have aligned to promote growth supportive reforms with adequate safeguards. In this context, the role of regulations in spurring innovations and ensuring financial stability is critical, which is an age-old debate that I shall try to delve into in detail in this part of my speech.

Right extent of Regulation in spurring innovations while ensuring financial stability

Regulation introduces both monetary and opportunity costs, requiring businesses to allocate funds to ensure compliance and often resulting in missed entrepreneurial opportunities. Hence, regulations need careful evaluation to ensure they achieve their social objectives at the lowest possible cost without stifling creativity, innovation or healthy market dynamics. Simultaneously, an overemphasis on innovation and competition without proper safeguards can lead to financial instability, resource misallocation and erosion of trust in the system.

The financial sector and its regulatory landscape are evolving rapidly, with emerging risks arising from new-age financial instruments and increased use of technology. The regulators in advanced economies provide assessment of compliance costs vis-à-vis intended benefits along with clear and definitive timelines, to ensure an informed decision-making in regulatory arena in transparent and efficient manner.

While ensuring stability of financial system remains the primary responsibility of regulatory framework, it is equally important to evaluate regulatory measures in terms of the associated cost and intended benefits. A robust compliance structure requires transparency in assessment and disclosure of compliance cost with definitive implementation timelines. As India's financial sector continues to expand, it is essential to ensure that the cost of compliance is commensurate with the intended benefits.

We need to be mindful of the five-pillar strategy of regulation – forward looking and proactive; nimble; data driven and impact assessment oriented; consultative approach; and collaboration with stakeholders.

Balancing regulatory quality is crucial for India's vast and diverse economy, its growing aspirations of Viksit Bharat and the significant investments required to sustain high growth and development. Globally, five key criteria are used to evaluate regulatory quality in an economy – democratic legitimacy; regulator accountability; fair and accessible procedures; expertise; and efficiency.

Since 2014, India has accelerated its regulatory reforms, simplifying taxation laws, rationalising labour regulations and decriminalising business laws to improve global competitiveness through grassroots-level structural changes. Regulation must consistently strive to find this equilibrium, implementing the reforms to maintain a balance that fosters growth while safeguarding the economy.

As banks are entrusted with the responsibility of serving society with sensitivity and inclusivity, they must always consider the needs of the people they serve, especially the vulnerable sections of society. Banks as well as bankers need to strengthen the inherent trust and integrity quotient of the general public. As trust bearers of society, our approach needs to be ethical, inclusive, responsible and prudent.

To keep pace within the guardrails of safety in the ever-evolving dynamic banking landscape, adopting and adapting right amount of regulation is crucial. It is well understood that banking regulation relies on pre-specified, time-tested and globally adopted toolkits like Basel Accords which indeed play a crucial role in shaping global banking regulations, much like a guiding text. These accords, established by the Basel Committee on Banking Supervision, provide comprehensive guidelines for banks to manage risks and ensure financial stability. Their standards, such as Basel I, Basel II and Basel III, have been instrumental in promoting sound risk management practices and maintaining confidence in the financial system worldwide.

In a rapidly evolving financial system, over reliance on existing regulation poses many potential challenges to the financial sector which are unforeseeable. Over the years, the sectoral dynamism has tested all regulations and every financial crisis has offered valuable insights, leading to modifications in these toolkits based on lessons learned.

Risk that seemed insignificant yesterday is quickly getting intensified today, posing threats to the

stability of the financial system. Take the case of online scamming through digital arrest. The speed at which it spreads and damages the system was never anticipated till it struck. Therefore, we must remain vigilant and responsive to all financial changes occurring around us.

Present and future regulations should adopt a differentiated regulatory mechanism based on the size, complexity and contribution to the systemic risk. As the interconnectedness, scope of activities and harmonization of financial intermediation increase, an entity-based regulatory architecture may lead to arbitrage between different entities undertaking similar activities. Therefore, moving forward, regulatory thought should focus on activities as a common framework for future regulations.

One-size-fit regulation approach carries a great uncertainty in the current regime. A closer look at regulatory landscape highlights the core principles upon which it is framed. In the Indian financial sector, the debate between Principle-based vis-à-vis Prescriptive (or rule based) regulations centres on the best approach to ensure financial stability while fostering innovation and flexibility.

While Principle-based regulations offer a flexible framework that guides behaviour through broad principles and objectives, it allows banks to apply these principles in ways that best fit their unique operations and circumstances. This approach encourages innovation in risk management and operational practices, as banks have the freedom to determine how to achieve regulatory objectives. The emphasis is on achieving desired outcomes, such as financial stability and ethical conduct, rather than strictly adhering to detailed rules. However, this flexibility can lead to variability in compliance and enforcement, as banks and regulators may interpret principles differently.

In contrast, Prescriptive regulation involves setting specific, detailed rules that banks must follow. This approach offers clarity and consistency, making it easier for banks to understand and comply with regulatory expectations. The predictability of Prescriptive regulations allows banks to plan their operations with certainty, reducing ambiguity. However, this rigid approach can stifle innovation, as it may not account for unique situations or evolving financial practices. Banks may find it challenging to adapt within the confines of strict rules, potentially leading to inefficiencies and missed opportunities for growth.

In summary, Prescriptive regulation in Indian banking offers clarity, consistency and predictability but can be rigid and limit innovation. Principle-based regulation provides flexibility and encourages innovation but may lead to variability in compliance and enforcement. The challenge for regulators is to strike the right balance between these approaches to ensure a stable, efficient and innovative banking sector that can adapt to changing market conditions and foster sustainable growth. Each approach has its benefits and is often chosen based on the regulatory environment and the nature of the financial system. The key is finding the right balance between flexibility and consistency to ensure a stable and innovative banking sector.

In the financial sector, regulations should strike an optimal balance between stability and fostering innovation, efficiency and competition. By rationalising regulations and aligning them with international standards, India can accelerate economic growth and employment, especially in the face of unprecedented global challenges. Regulators in India must consistently strive to find this equilibrium, implementing the reforms to maintain a balance that fosters growth while safeguarding the economy.

Thank you once again Indian Institute of Banking & Finance (IIBF) for organising this lecture and giving me an opportunity to share my thoughts. Also, thanks to all the distinguished guests for your patient listening.

Thank you all!

FROM FIXING POINTS OF INSTABILITY TO SETTING A STATE OF RESILIENCE MAKING FINANCIAL ENTITIES "DISTRESS-IMMUNE" & "FUTURE-READY"

Dr. Rabi Narayan Mishra*

The Past and The Present

There were important lessons learnt from the Global Financial Crisis (GFC) 2008-09. Many jurisdictions, including India had undertaken lots of reforms thereafter to ensure that the associated fault lines are fixed so that crisis of that magnitude and intensity does not recur.

The following lessons were taken up seriously to be addressed in India in particular:

- **Stability breeds Financial Instability**

  A sustained state of macro-financial stability makes the stakeholders complacent enough to dilute standards of business related decision-making, thus, creating scope for instability showing up at different points of the entities and the economy.

- **Novel Innovations in Financial sector**

  With rapid growth and use of technology, path breaking innovations were observed in the financial space but those were not well-tested for their long-term utility.

- **Mushrooming growth of Financial products**

  Innovations were oriented towards creating structured products for rising pace of business growth while circumventing on requirements of risk capital there against.

- **Impact of Systemic Risk on Individual Entities & Vice Versa**

  There was observed perceptible impact of the state of macroeconomic system on the health of individual financial entities and vice versa.

- **Interconnectedness – Spillover Effects**

  There were inter-sectoral, intra-sectoral and inter-economy interconnectedness resulting in spillover effects all over. This enabled problem in a small and new entity snowballing into a world-wide distress.

- **Fragile framework of Crisis Management**

  Systems to handle surfacing of crisis in entities as well as the entire financial space were either not existing or were observed to be inadequate.

- **Lax Financial Sector Regulation**

  With the use of new financial products by financial entities, their regulation was required to be stringent. But that was not the case in USA, UK and Europe.

- **Poor Enforcement actions**

  While regulatory violations were rampant, regulatory actions, including enforcement-oriented punishments were not in vogue.

- **Less Intense Financial Sector Supervision**

  Worst of it, with all these happening all around the financial space, instead of intensifying the rigours of supervision, supervisors did not rise of the need of the hour.

Fixing the Fault lines

Based on the understanding of each of such lessons, a menu of post-GFC reforms measures were spelt

*Director, College of Supervisors, Reserve Bank of India.
Dr. Mishra is the former Executive Director (Supervision & SupTech). He was the founder Head of Financial Stability Department and the Head of Risk Monitoring Department at RBI too. He is a reputed Economist being a Fellow of Economics Department of Harvard University, USA. He is a 'Diamond Jubilee & CH Bhabha Banking Overseas Research Fellowship' Fellow of the IIBF.

An abridged version of the Transcript of the Lecture.

out by international organisations like (Bank for International Settlements (BIS) and the Financial Stability Board. India, as usual, remained acutely conscious and active in their implementation and execution.

Some of those reforms are as under:

Reconfiguring Regulatory Philosophy

From Sector Agnostic to Sector Specific Regulation

- Regulations tailored to unique sectoral characteristics.

Addressing Pro-Cyclical Features

- Control risks such as shifts in loan-to-value ratios in housing markets.

Addressing Too Complex to Fail

- Focus on Size + Complexity + Interconnectedness of institutions.

Migration of Risks

- Prevent risks from migrating to poorly regulated or unregulated areas.

Ensuring more capital and less leverage.

Maintain high-quality liquid assets and stable funding sources.

Understanding Systemic Risk and Interconnectedness

- Recognize how systemic risks propagate.

Macroprudential Regulations

- Strengthen regulations to address systemic risks.

Re-Tooling Supervisory Armory

Relook at Supervision

- Holistic, all-pervasive and ongoing supervision.

More Intensified Off-Site Surveillance (OSS) and On-Site Examination tailored to look at

- Bank-specific risks
- Risk-specific issues
- Portfolio-specific exposures

Measuring Interconnectedness

- Inter-sectoral, Intra-sectoral and Inter-economy linkages.

Identifying Vulnerable Institutions

- Pinpointing institutions with high exposure to risks.

Early Warning Mechanism

- Systems to detect vulnerabilities early and intervene effectively.

Forward-Looking Stress Testing Framework

- Simulations to identify future risks under adverse scenarios.

Understanding Global policy/crisis spillovers

- Assess spillover effects of global financial policies.

Global Coordination architecture

- Collaborative framework for monetary and financial stability policymaking.

The Future

With this background on the past and present, it is appropriate to flag off important issues for the Future.

'Stability' is good, but 'Resilience' is the Goal

Absence of instability is stability. Points of distress in any corner of the financial system, macro economy, financial entities, financial markets and financial infrastructure are viewed as precursors to instability in the system. Each of these units within a system being interconnected, distress anywhere could snowball into instability everywhere (or in the whole system).

Distress is an aberration from historical performance manifested in malfunction. Instability is a continued state of distress crying for redressal. Steps are taken to redress state of instability by overhauling the perceived fault lines by virtue of using cutting edge tools and techniques. A state of stability is, thus, achieved. If the tools and techniques are intelligently

used to ensure that the same fault lines do not recur and the associated difficulties are identified and solutions found; it could bring about a sustained state of stability, which can be defined as achieving resilience.

Hence, making macroeconomy, individual entities, market & infrastructure resilient and the system resilient is THE solution.

Time to redefine Resilience

Operational Resilience - OR.2

The risks out of critical operations, products and processes are the most-fickle. Each of these should be identified afresh at each and every business units and be re-categorised as known-known, known-unknown and unknown-unknown risks.

The fickleness of each of these risks-emitting items of processes and products should warrant the intensity of management attention and proactive action. The possible points of distress should be smelt and be nipped in the bud. Simulation exercises as pilots would reinforce integrity of the mechanics of NewGen OR.2.

Most importantly, this re-engineering should be jointly shouldered by Chief Risk Officer (CRO), Chief Compliance Officer (CCO) & Head of Internal Audit and be operationalised by the members of the senior management based on a codified board approved policy document.

Functional Resilience - FR.2

Functional resilience refers to recognising and addressing the risks embodied in the way a financial entity functions.

Institutional culture of the way of functioning by its personnel at the levels of junior/middle management, senior management and top management including the Board and its Committees is the nucleus of a Functional Resilience Framework.

How synchronised are the Tone from the Top, the Whispers in the Middle and the Rumblings at the Bottom is a very crucial variable that can make or mar decision-making towards resilience. That too is a building block for such a framework.

Quality and loyalty of leadership, culture of ethical business conduct, corner rooms' professional & attitudinal symphony - all these are cornerstones of an effective Functional Resilience framework.

Quality of risks and assurance standards, deep dedication for compliance of regulatory, supervisory and internal control stipulations, empathetic employees engagement stipulations, gender inclusivity etc. are the other facets.

That all these are not static but need to constantly change in sync with dynamics of the economy must not be forgotten.

The mechanics and tools to achieve Functional Resilience is the challenge that needs to be addressed as fast as possible. Those too would change with time. After all, Dynamic resilience is the buzzword.

Financial Resilience - Fin R.2

The third leg of a resilient financial entity is Financial Resilience. Traditionally, it means having adequate liquidity and capital to meet any episode of distress.

Liquidity should be adequate enough to meet projected and some of unanticipated outflows.

Capital should be enough to keep the entity far away of any possibility of insolvency. The realisable value of assets should hence be more than those of liabilities at any point of time.

To be sure about a state of financial resilience, there are other important considerations to evaluate.

(a) Illiquidity can snowball into insolvency very fast. Rumours in social media have indeed hastened this process.

(b) There should be sufficient capital cushion available to meet unforeseen distress out of 'known-unknown' and 'unknown-unknown' risks as well.

The extant resilience exercise, however, remains

limited to evaluate capital provisions for 'known-known' risks only. That means, in the absence of measuring and allocating capital to all possible risks, the entity remains prone to distress and hence, definitionally should not be thought to be "resilient".

This lay bare another interesting facet of running entities. That is, without being clear about how far the entity is from the real quantum of deficit of risk capital which is the reflection on the reality on its state of resilience, 'compensation' is calculated and distributed as an expenditure and net profit is announced.

That 'number of net profit' is illusory since the entity is still to achieve 'financial resilience' in the truest sense of the term.

Time to appreciate: Risk and Uncertainty – Two sides of the same coin?

The game of finance is characteristically quite tricky as Napoleon Bonaparte had said "Money has no motherland; financiers are without patriotism and without decency; their sole object is gain". In this game, risk is the raw material. Any potential uncertainty that could materialize into an 'issue' in the foreseeable future is branded as "Risk" and the best way to handle it would be to have a knack for smelling or sixth-sensing their possible occurrence.

Warren Buffet has very rightly described risk saying "Risk comes from not knowing what you are doing". So, the knowledge of risk and sensitiveness to their occurrence are the minimum "basics" that everyone in the game of finance must learn. Though risks follow rewards in terms of higher interest margins, the tendency to carry a level of risk that could jeopardize the ability to meet the liabilities to depositors and other stakeholders needs to be shunned. Interestingly, as has been mentioned earlier, stability breeds instability as there is a tendency to increase risk exposure during stable times to earn a higher margin and get off-guard when a crisis hit.

Distress, instability and crisis are the various stages of a downhill trip in the Game of Finance. Post-COVID-19, the regular world of VUCA - Volatility, Uncertainty, Complexity and Ambiguity – found itself in a much worse situation. With fear and uncertainty on the rise, people tended to overreact and refrained from initiating or following through even routine transactions and economic activities. "Unknown-unknown risk" amidst a kind of "Knightian uncertainty"[1] attempted to overpower business sentiments. "Catastrophizing"[2] - which contribute to the worsening of the intensity of such uncertainty became the popular narrative.

This resulted in a Rooseveltian fear of fear itself. A fear to the power of infinity. The risks facing individuals, businesses and the economy, at present are, at least to some degree, within our control, collectively if not individually. All these risks can be mitigated, if not eliminated entirely, by the actions of individuals, businesses and policymakers if they opt to stay with the troika of Adaptability, Agility & Sustainability. Therefore, there is an acute need to avoid the economics of 'Chicken Licken'[3]. We must learn to create a balanced narrative while describing the outlook on the financial landscape.

Preparing for Uncertainty - Scenario Planning – Boosting Self-immunity to distress

Financial entities should use Scenario planning as a tool to address uncertainty. Realistic and sensible assumptions will need to be made on 'what the future could look like, how the business environment might change and how the organization could respond to those changes'. Right tone from the Top will encourage such planning and thus could result in tangible action plan that demonstrates value rather than potentially becoming just another compliance activity to check-off.

The benefits from the conduct of rigorous scenario would accrue more if done on a structured format – say once a year – and should be undertaken in sync with updated risk-related inventories and concurrently

[1]Risks those are impossible to measure and hence manage.

[2]Psychologists define "catastrophizing" as – discounting the best and fixating on the worst, whatever the balance of risks.

[3]'Chicken Licken' fears anything and everything. One day, while he was sitting under a tree, an acorn fell on his head. Chicken Licken did see the acorn and started thinking that the sky must be falling. He decided that he must warn the King about such fall.

with dynamically redefined strategic plans. This way, the exercise could be made forward-looking while keeping on identifying strategic opportunities and the associated incremental risk appetite. Such planning could also be used as a useful tool for long-term strategic plan as it would use the stream of short-term decisions, tactical plans and intelligent learning outcomes as the parts of day-to-day running of businesses.

This way, besides improving the design of Early Warning System (EWS) and Stress testing mechanisms, the institutions should learn to improve their individual institutional immunity from shocks, of course, with the hand-holding of Supervisors.

Need to remain Risk-conscious and its "know-how" – Automated sophisticated Risk Management Systems might play havoc.

To understand this aspect, let me remind you of the tragic Aeroplane crash on May 31, 2009. 216 passengers, three pilots and nine flight attendants boarded Air France Flight 447 from Rio De Janeiro to Paris. Few hours into the flight, its autopilot suddenly disengaged itself. The pilots, unaware of the stalled plane coupled with lack of manual flying experience, made elementary but important errors in flying the plane.

The result was that plane crashed into the sea and everyone on board died.

In the aviation industry, there is a phrase used for pilots "Children of the Magenta" signifying that they have become over dependent on the magenta coloured guiding lines of automated flight systems for a safe flight and they may have difficulty flying without such assistance. The autopilot invention, of course, has substantially reduced the incidence of plane accidents, but absence of basic knowledge can still play havoc.

In the same vein, increased sophistication in the game of finance especially in risk management systems, means greater complexity (and therefore, greater scope for error), less transparency (making errors harder to detect) and greater dependence on underlying assumptions (any one of which could be wrong). A simple system might look primitive but is usually transparent and risk managers can easily get a sense of its strengths and weaknesses and can pay more attention to qualitative factors, to apply common sense over models while solving the judgmental questions surrounding them.

We need to believe that Risk Management models are not enough - Managerial application of mind is also essential.

There was an important lesson from GFC 2008-09. Despite the use of the sophisticated models, the rigours of stress testing and the vagaries of bottom line numbers, those who could come out unscathed were those having agile management, not those who relied on models to do the management's job. Risk models do have a valuable function in the risk management process so long as their limitations are recognized. They are useful in managing the risk in a trading desk, but not in capturing the risk of large divisions, not to mention the entire institution.

Managing systemic risk which reflects the aggregation of risks across the financial system relying solely on statistical models could prove to be a folly. We can, of course, get some numbers, but the numbers carry no understandable meaning. The global financial crisis provided a perfect example of emergent risks and the challenges of getting prepared for them. More broadly, dealing with emergent phenomena requires attention to what is possible, rather than the probabilities of possibilities and strategies of resilience, robustness and responsiveness.

Hence, there is a need to ensure that the risk impact of the pandemic is fully analysed and understood by the organisations and they opt to redesign their Risk Management architecture.

Colour, Contour and Characteristics of Risk are fast changing

The way specific risk management activities have been performed over the past 25 years is now almost

redundant. While it is culturally challenging to accept this, the need to re-tool and take a different approach to risk management while responsibly leading employees through the change.

Top Risks for 2030
1. Adoption of digital technologies may require new skills that are in short supply.
2. Impact of regulatory change and scrutiny on operational resilience, products and services.
3. Rapid speed of disruptive innovation may outpace the ability to compete.
4. Leadership succession challenges: ability to attract and retain talent.
5. Privacy, identity management and information security challenges.
6. Substitute products or services may arise that affect our business model.
7. Sustaining customer loyalty and retention may be difficult as preferences and demographic shifts evolve.
8. Ability to compete with "born digital" and other competitors.
9. Ability to utilize data analytics and big data to achieve market intelligence and increase efficiency.
10. Cyber threats.

Four risks on the top 10 list for 2030 were not on the top 10 list for the last decade.

More significantly, the risk which was ranked 18 in 2021, jumped to the third-ranked risk for 2030.

The rapid speed of disruptive innovations enabled by new and emerging technologies (e.g. Artificial Intelligence (AI), automation, machine learning, hyper-scalable platforms and increasing bandwidth through 5G data transmission) and/or other market forces are outpacing an organization's ability to compete without making significant changes to its business model.

The overarching theme is the unprecedented and accelerated changes in disruptive innovations over the next 10 years. This may drastically alter customer behaviour. Customer loyalty is likely to prove fleeting as preferences and demographic shifts evolve. New markets and competitors offering alternative products and services are expected to expand customer choice in ways that could affect the viability of current business models and planned strategic initiatives. In sync with these, the architecture of risk management must also change.

The current way of doing things had to change.

Quick suggestion from my side –

- Getting the first line of defense more involved in risk identification should be the priority. To a survey question "how many of your firms see more than 50% of your issues or risks identified by the first line of defense"? Approximately 20% of attendees raised their hands.

  To improve this position, there is a need to remove associated cultural and technological impediments which will require creative solutions.
- Risk management is a menu of a few activities – risk identification, risk measurement and creative solutions to manage risk effectively. These are embryonically inter-linked.

Risk Managers should be masters in all these together - not one or the other.

Of course, redesigning or reconfiguring risk management architecture is a journey - not a destination. The Risk Managers should, however, not lose sight of the exact route to be taken at the right point of time.

Planning for "Known-Unknowns" is necessary but smelling "Unknown-Unknowns" will be the winners' traits.

"There are known-knowns; there are things we know we know. We also know there are known-unknowns; we know there are some things we do not know. But there are also unknown-unknowns – the ones we do not know we do not know."

Former United States Secretary of Defense, Mr. Donald Rumsfeld made this complex statement at a press conference on 12th February 2002 when he announced that there was no evidence that Iraq was supplying weapons of mass destruction to terrorist groups.

In risk management too, Risk Managers will need to deal with the "known-unknowns" and the "unknown-unknowns".

'Known-knowns' are assumptions that have been validated and are now facts. But, known-knowns are not necessarily static. They could change over even a short span of time – possibly even during the period when the project is still live – scenarios might change – compulsions might raise their head - significant change in the scope, cost or schedule may happen. Such potential risks might require attention, identification, re-measurement and careful monitoring.

Unknown-unknowns are true surprises. They follow Murphey's Law. These are "silent assassins" because we do not recognize them until it is too late. These are usually shared through lessons learned for future risk consideration for projects as a known-unknown. Assumptions are important in such cases. Risk Managers should be able to visualize them, smell them, if possible see them, rate them and resolve them so much so that the conclusions drawn and the policy making that follows do not turn out to be non-sense as they pan out.

The big job, hence, is to ensure that all the staff are engaged with what is required from a risk management perspective and that their actions are being monitored. This means that a culture of risk awareness in the last mile needs to be inculcated.

Risk-Acculturisation measures should enable each member to smell the risk in advance and alert the Risk Marshalls. This will ensure the organisation to remain "risk intelligent" not just "risk aware/conscious". All should remain clear about the company's risk strategy and governance.

The role of Risk Managers should, thus, be expanded from being Business silos to holistic Balance sheet management.

Risk Intelligence should flow from the Top. Discussion on Risk should be a fixed agenda for any Top Management meetings on strategic decision-making. There should be complete transparency on the kinds and levels risk underlying the business activities – small or big. Each worker should be a Risk Manager for his job responsibilities with clear accountability provisions. In short, Risk Intelligence should be a part of the DNA of the organisation.

Rigours of risk management should be symmetric across all the Business units – Be it Enterprise Wide and not Silo-based with a narrow focus. Interconnectedness of risks are difficult to anticipate or perceive but there should be ways to be able to measure them and include them as a part of the Risk evaluation exercise. Without this, potential threats to the business will be perennially there as a Damocles' sword hanging around.

The role of risk management should shift from an 'offensive type' to a 'defensive type'. Offensive risk management aims to leverage risk to raise profits and hence, shareholders value, whereas, Defensive risk management professes to create a 'crisis-prepared' environment which would reduce the probabilities of distress so much that the direction of profits would remain positive on a sustained basis and so are the confidence of the shareholders on their value.

The former is short-term while the latter is for the long-term.

As such, Disconnected risk management based on 'returns from the silos' may have other negative externalities in the nature of regulatory fines, unforeseen liabilities and even the failure of that silo business which can get the whole organisation on its kneels.

Plan to create a resilient financial entity? Neither 100-meter race nor a marathon should be the strategy.

Creating a financial entity is not a destination but a journey. That is well understood. But the strategy to be adopted to start creating a resilient one is viewed differently by different experts. Some go with 'slow

and steady' while few others believe in a 'Big Bang approach'.

It should, however, be best to follow a sweet hybrid framework.

A tight timeline should be framed and followed to start working while dealing with teething problems. Each year starting with the maiden one should end with tangible performance milestones. Provision of years or months of working should not be kept for to 'test the waters' but every day should lead to few hours of performance. There should not be any leisure time to 'stand and stare'.

Every hour should be a race for '100 meters' towards a 'marathon race for 100 years'.

Building an Institution could be a child's play for 'some' but creating a resilient institution that too a financial one is a complex job that warrants lots of efforts 'for everyone'.

Let me pepper the "Thoughts for Future" with some practical suggestions to achieve them.

1. Chief Risk Officers (CROs) should be able to develop a collaborative relationship with business line leaders. They should be very strong in their interpersonal skills to achieve effective relationships and motivating others. For that to happen, they must be cool under fire.
2. They should gain free access to the board for conveyance and reporting. Not providing such access would cause disconnect in communication and the loss of resolutions to various strategic problems.
3. They should be skilled at Strategic thinking, effective analysis of data and the ability to disaggregate business plans into component risks.
4. They should have a strong understanding of processes and core management activities.
5. Risk appetite should be clearly understood and be codified.

While doing so, three points should be carefully considered.

(a) The capability to incubate new products which can trace the potentials for possible opportunity gains. These are the incremental strategic alternatives which could be considered at a particular point of time.

(b) The finesses with which those could be executed with lowest possible gestation periods. This can, thus, control cost.

(c) These are in accordance with the avowed character and devised goals of the organization as crafted by the Board members and the Heads of various Business units.

6. Boosting Self-Resilience by the Entities
   - Identify brewing risks – Known-unknowns
   - Have a measurable index
   - Discuss with the concerned Business head
   - Escalate it to Chief Executive Officer-Risk Management Committee (CEO-RMC)
   - Have a contingency plan
   - Create organisation-wide awareness
7. Configure entity-specific empirical models
   - Risk Dossiers for each business
   - Early warning indicators
   - Forward looking Stress test framework
8. Identification of Vulnerable businesses & borrowers/counterparties through quantifiable institution-specific models
9. Measuring interconnected risk
10. Managing 'Similar models risks"
11. Recognising and working on measures to handle newer risks
    - Climate risk
    - Vendors' risk
    - Digital platform/Business model risk
    - Conduct risk

- Moral hazard risk
- Reputation risk
- Technology risk
- Outsourcing risk

12. Keeping ready an effective Operational Resilience plan
13. Preserving reserves for the rainy days

It will be worthwhile to end with the following with two quotes.

- James Lam - a global expert on Enterprise Risk Management (ERM) – "The only alternative to risk management is crisis management - and crisis management is much more expensive, time consuming and embarrassing".
- Robert Heinlein: "People do not learn from the mistakes of others. They seldom learn from their own mistakes. Never underestimate the power of human stupidity".

STATEMENT ABOUT OWNERSHIP AND OTHER PARTICULARS OF BANK QUEST, THE JOURNAL OF INDIAN INSTITUTE OF BANKING & FINANCE

1.	Place of Publication	:	Mumbai
2.	Periodicity of Publication	:	Quarterly
3.	Publisher's Name	:	Mr. Biswa Ketan Das
	Nationality	:	Indian
	Address	:	Indian Institute of Banking & Finance Kohinoor City, Commercial-II, Tower-1, Kirol Road, Kurla (W), Mumbai-400 070.
4.	Editor's Name	:	Mr. Biswa Ketan Das
	Nationality	:	Indian
	Address	:	Indian Institute of Banking & Finance Kohinoor City, Commercial-II, Tower-1, Kirol Road, Kurla (W), Mumbai-400 070.
5.	Name of Printing Press	:	Onlooker Press, A2, Byculla Service Industries, Dadoji Konddeo Road, Byculla (E), Mumbai-400 027.
6.	The name and Address of the Owners	:	Indian Institute of Banking & Finance Kohinoor City, Commercial-II, Tower-1, Kirol Road, Kurla (W), Mumbai-400 070.

I, Biswa Ketan Das, hereby declare that the particulars given above are true to the best of my knowledge and belief.

31.03.2025

Biswa Ketan Das
Signature of Publisher

REPORT ON 21st APABI INTERNATIONAL CONFERENCE 2024

The 21st biennial International conference 2024 of the Asian-Pacific Association of Banking Institutes (APABI) has been organized successfully by the Indian Institute of Banking & Finance (IIBF) on 14th November (Thursday) at the Hotel Taj President, Mumbai. The conference was attended by Senior Executives from the Banking Institutes across Asia-Pacific region, e.g. South Korea, Philippines, Malaysia, Vietnam, Cambodia, Nepal, Bhutan, Mongolia etc., along with senior bankers from public sector & private sector banks in India. The theme for the conference was "Paradigm shift in Banking: Moving towards a resilient, inclusive & sustainable model".

The aim of the conference was to bring together educators, industry experts and senior Banking, Financial Services and Insurance (BFSI) professionals from the Asia-Pacific nations on a common podium, so as to learn from their perspectives and vast experiences in a thought-provoking environment. The theme of the conference was specifically chosen to promote exchange of ideas and share best practices in banking education among peer institutes. IIBF, a pioneer in BFSI education in India for the last 97-years and an alma mater for most of the banking professionals in India today, played the appropriate host.

The conference had an auspicious beginning with the traditional prayer and the lighting of the lamp.

Shri Biswa Ketan Das, Chief Executive Officer (CEO), Indian Institute of Banking & Finance (IIBF) extended a warm welcome to the international and national dignitaries to the conference. He then touched upon the proud legacy of IIBF and set the scene for further deliberations on the theme of the conference by highlighting on the immediate need of upskilling and reskilling to nurture the human capital in a fast-evolving banking ecosystem.

The inaugural address, delivered virtually by Shri Atul Kumar Goel, Managing Director (MD) & CEO, Punjab National Bank and President, IIBF, duly focused on the importance of staying inclusive and resilient in the face of the paradigm shift brought about by fast technological advancements and rapid innovation, to ensure the requisite quality of customer service in banks. Shri Goel has duly highlighted on the importance of inclusivity and financial literacy in banking, by empowering individuals through innovations. He focused on the importance of acknowledging and incorporating climate considerations in the credit appraisal and underwriting process to ensure sustainable banking practices. Shri Goel has also congratulated the APABI members for working cohesively towards a brighter future.

Shri Mahendra Dohare, Executive Director, Central Bank of India, has also highlighted on the importance of capacity building and reskilling & upskilling of bankers to navigate the changing face of BFSI ecosystem. He also focused on the importance of bringing in the climate considerations to ensure sustainability and resilience. Shri Dohare has also highlighted on the pioneering role played by IIBF in the domain of banking education in India and congratulated it for the upcoming centenary.

Shri Gopal Murli Bhagat, Deputy Chief Executive, Indian Banks' Association (IBA), deliberated upon the role played by IBA in bringing together the banks in India to counter the systemic issues and challenges in banking, like the pandemic. He brought forth the importance of 'digital-first' approach to increase the resilience & inclusivity in banking. He emphasized on the importance of sustainability and the need to decrease the carbon intensity of banks' portfolios to ensure sustainability and resilience. He congratulated IIBF for bringing together the members of APABI to deliberate upon such key issues.

The keynote address by Smt. Charulatha S. Kar, Executive Director, Reserve Bank of India (RBI), focused on the importance of capacity building to counter the pressing challenges in banking, especially the paradigm shifts brought about technological innovations. She highlighted the importance of staying agile in the face of rapid changes across the banking ecosystem, to provide a tailored and digitized customer journey by leveraging on recent advancements like artificial intelligence, machine learning & blockchain-based Application Programming Interfaces (APIs). She also highlighted on the recent Government initiatives like Pradhan Mantri Jan Dhan Yojana (PMJDY) to promote financial inclusion and also mentioned the recent initiative of 'Unified Lending Interface' to ensure frictionless credit to all. RBI's recent measures, like regulatory sandbox and engagement with FinTechs to promote controlled innovations in digital solutions in banking space have been duly mentioned by her to ensure data security and prevent cybercrimes. Finally, Smt. Kar has deliberated on the measures taken to ensure sustainability in the banking domain by cutting down on carbon footprints. She ended her speech by focusing on HR transformation, targeted learning and capacity building programmes to develop new skillsets in nurturing future leaders in the industry and complemented IIBF for its pioneering role in the capacity building space in India.

The speeches were followed by four highly engaging and insightful panel discussions wherein international and national experts exchanged their ideas,

experiences across geographies and shared valuable inputs in terms of developing the human capital to adapt and progress to the evolving BFSI ecosystem.

The first panel discussion was conducted on the topic of "Empowering through knowledge- Preparing future ready banking professionals". The panel consisted of Ms. Wan-Hsin Huang, AVP & Head of Financial Training Group, Taiwan Academy of Banking & Finance (TABF); Smt. Suranjana Dutta, Chief General Manager (CGM) & Head-Strategic Training Unit (STU), State Bank of India; Dr. Chetna Pandey, General Manager-Learning & Development, Union Bank of India and Prof. Srinivasan R. Iyengar, former Director-Jamnalal Bajaj Institute of Management Studies (JBIMS). The panel was insightfully moderated by Dr. K. Gangadharan, Director (Academics), IIBF. Shri Krishan Mishra, CEO, FPSB-India, established the context of the panel discussion through his brief yet insightful speech on the importance of professional education and continuous learning. The panel deliberated in detail upon the paramount importance of nurturing the human capital. Ms. Huang talked about banks' growing investments in generative AI technology. Smt. Dutta talked about challenging the status quo through continuous knowledge. Dr. Pandey talked about fulfilling leadership gaps through upskilling and continuous learning. Prof. Srinivasan, on his turn, talked about knowledge-driven business models. The panel agreed on the immediate need for investing in human capital, leveraging on the technology-driven pedagogies, personalised learning solutions and increased collaboration between industry & academic institutes. The panel also indicated the need for joint research initiatives and industry-focused curriculum.

The second panel discussion focused on the important topic of "Digital Transformation: Redefining the Banking Landscape". Shri Rajeev Ranjan Prasad, Chief General Manager (CGM)-Digital Banking, State Bank of India, laid the context through his detailed presentation on the digital disruption & subsequent transformation of the banking system in India, especially in the digital lending & remittance domains. The panel, thereafter, focused on the digital transformation perspectives from other geographies through deliberations from Ms. Carrie Leung, CEO, The Hong Kong Institute of Bankers (HKIB) and Mr. SOU Visal, CEO, Institute of Banking & Finance (IBF) Cambodia, Shri Suresh Shankaran, Senior Vice President-Information Security Group (SVP-ISG), HDFC Bank and Shri E. Ratan Kumar, General Manager-Information Technology (GM-IT), Central Bank of India, put forth the transformational perspective in India. The panel was moderated by Shri LVR Prasad, Director (Training), IIBF. The panel deliberated upon the crucial need to improve customer experiences by leveraging technology, while not compromising on the data security perspective. The panel envisaged that increased collaboration with FinTech companies to improve customer onboarding and relationship experiences would be crucial for banks in the days to come. The panel also saw digital collaborations to be a critical strategy to ensure financial inclusion going forward. The panel concluded on the importance of customer education for ensuring digital security.

The third panel focused on the crucial topic of "Climate Risk & Sustainable Finance-Challenges & Opportunities". The panel was made up of Smt. Shobana Chawla, Executive Director (ED), Standard Chartered Bank; Shri Ankit Jain, CEO, StepChange; Shri V Chandrasekar, Senior Advisor- Corporate & International Banking (C&IB), Indian Banks' Association (IBA) and Shri Ashutosh Tandon, FIG Advisory Officer-South Asia, International Finance Corporation. The discussions were moderated by Shri Biswa Ketan Das, CEO, IIBF. The topic was introduced by Shri Sunil T S Nair, Chief General Manager (CGM), Reserve Bank of India through an insightful speech on the need for incorporating climate risks in the risk management processes of banks and highlighted on

the RBI initiative to address the issue of unavailability of standardized & reliable climate data through introduction of 'RB-CRIS', a climate data repository for India. The panel, on its turn, has deliberated in detail about the importance of factoring climate risks in the credit appraisal and underwriting process of a Bank, of calculating the Bank's emissions including financed emissions and to disclose the emissions in an effective and trustworthy manner. The panel has deep-dived on the impact of Carbon Border Adjustment Mechanism (CBAM) or similar carbon taxes on India's exports and has also touched upon the necessity of introducing an effective carbon trading market for financing the transition. Moreover, the panel deliberated on the human-side of climate adaptation processes and the importance of funding such initiatives. At the end, the panel has highlighted on the importance of creating the relevant capacity amongst the employees of banks across levels, to create the necessary awareness on climate-related risks and mitigations.

As a guest speaker, Mr. Simon Thomson from the Global Capacity Building Coalition, has called for prioritising the capacity building initiatives across the globe to tackle climate change more effectively.

The fourth and final panel deliberated on the topic of "Data driven Banking: Leveraging Big data and Artificial Intelligence". Shri Balaji Rajagopalan, Chief Technology Officer (CTO), State Bank of India provided some valuable insights on the aspect of effective data mining for excellence in customer experiences, followed by a detailed discussion by the panel moderated by Dr. Narinder Bhasin, Head-Professional Development Centre, Northern Zone (PDC NZ), IIBF. The panel was made up of Mr. Reginald C. Nery, Senior Vice President and Chief Audit Executive, Bankers Institute of Phillipines; Shri Rajesh Kumar Ram, General Manager (GM)-Digital Banking, Bank of India; Shri Jalpesh Shah, Head-Data Science, Credit Analytics & Innovation, HDFC Bank and Shri Burra Butchi Babu, IT advisory board member, Punjab & Sind Bank. The panel discussed the need to incorporate effective data governance models for managing the huge volume of available data ethically and prudently. The panel highlighted the importance of adequate domain knowledge to modulate the data management tools, to create multifunctional data models. The panel has mentioned the need of reskilling and upskilling for existing employees on the areas of big data and artificial intelligence. The panel was unanimous in ensuring data security and ethical data usage to prevent transactional frauds and cyber-threats. The panel concluded by saying that the regulatory framework is required to catch up with the path-breaking developments in the domain, while we move towards a data-driven banking model.

As a part of the conference, the Institute also released its special issue of the 'Bank Quest' on the theme of the conference covering articles on new paradigms in banking penned by Indian and International authors, including senior-most executives from banks & Financial Institutions (FIs) in India, which gave national and global perspectives on banking issues.

39th Sir Purshotamdas Thakurdas Memorial Lecture

The prestigious Sir Purshotamdas Thakurdas Memorial lecture (39th lecture) was delivered by Dr. Rabi Narayan Mishra, Director, College of Supervisors, Reserve Bank of India on the topic of "From fixing points of instability to setting a state of resilience: Making financial entities distress-immune and future-ready".

Dr. Mishra started his insightful delivery with the epiphet that 'Stability breeds instability', therefore, a prolonged period of stability needs to monitored thoroughly for inherent systemic risks. Moreover, the era of financial innovations has led to a mushrooming growth of financial products, thereby, increasing the systemic risks in exponentially in an interconnected

monetary system worldwide. Resilience of the financial system is synonymous with a sustained state of stability, as he appropriately deliberated. Dr. Mishra has insightfully divided the risks that the financial system faces, into three areas: 'known-known risks', 'known-unknown risks' and 'unknown-unknown risks'. Addressing these risks, in turn, are closely related to the overall resilience of the financial system.

Dr. Mishra has deliberated upon the three different types of resilience that an organization needs to ensure in order to become truly resilient, namely financial resilience, operational resilience and functional resilience. Dr. Mishra has highlighted on the importance of relooking at the existing regulations and has called to move from sector-agnostic regulations to sector-specific regulations.

Dr. Mishra has emphasized on the critical role of an organization like IIBF for propagation of necessary awareness and knowledge-base for the banking community as a whole, in the critical aspect of increasing resilience in the banking ecosystem.

Dr. Mishra has concluded his address with the very pertinent argument that every CEO needs to be focusing on building their systems & processes in such a way that natural resilience is created within the system. In that way, the internal system can predict in advance and effectively deal with crises or any adverse event, as and when they arise.

21st APABI International Conference 2024

21st APABI International Conference 2024 - 14th November 2024: Welcome Address by Mr. Biswa Ketan Das, CEO, IIBF

Inaugural session- (L-R): Mr. Biswa Ketan Das, Chief Executive Officer; Smt. Charulatha S. Kar, Executive Director, Reserve Bank of India; Mr. Mahendra Dohare, Executive Director, Central Bank of India; Mr. Gopal Murli Bhagat, Deputy Chief Executive, Indian Banks' Association

Mr. Biswa Ketan Das, CEO, IIBF moderating the Panel Discussion

MITIGATING CYBER THREATS IN THE BFSI SECTOR: AI-DRIVEN RISK MANAGEMENT AND RESILIENCE STRATEGIES

Dr. Sachin Sharma*

Mukesh Ahuja**

Abstract

The Banking, Financial Services and Insurance (BFSI) sector faces escalating cyber security challenges due to the rapid digital transformation and increasing sophistication of cyber threats. This paper explores the evolving threat landscape and emphasizes the transformative potential of Artificial Intelligence (AI) in enhancing cyber risk management and organizational resilience. It presents a comprehensive analysis of AI-driven cyber security approaches, including anomaly detection, fraud prevention, automated incident response and behavioural analytics. The study contrasts traditional and AI-enabled strategies, highlighting the limitations of legacy systems and the benefits of AI-powered Security Orchestration, Automation and Response (SOAR) platforms. Real-world case studies and industry implementations illustrate how leading financial institutions leverage AI for predictive analytics and adaptive defense mechanisms. Furthermore, the paper examines the regulatory landscape, adoption challenges and future directions, emphasizing the integration of AI with Zero Trust frameworks and digital banking platforms. The findings provide actionable insights for BFSI institutions to strengthen their cyber security posture, ensure regulatory compliance and build robust, intelligent and future-ready risk management systems.

Introduction

In recent years, the Banking, Financial Services and Insurance (BFSI) sector has become a prime target for cyber attacks due to its critical role in managing sensitive financial data and transactions. As financial institutions increasingly digitize their operations, the need for robust cyber security measures has never been more urgent (Sharma & Kumar, 2022). The rising sophistication and frequency of cyber threats pose significant challenges to the sector, prompting a call for innovative solutions to ensure business continuity, data protection and operational resilience. This section explores the importance of cyber security in the BFSI sector, the escalating nature of cyber threats, the pivotal role of Artificial Intelligence (AI) and other advanced technologies in enhancing cyber security and the objective of this article, which is to analyze AI-driven strategies for effective cyber risk management.

Importance of Cyber security in the BFSI sector

Cyber security is fundamental to maintain the trust and integrity of financial system. The BFSI sector handles vast amount of sensitive personal, corporate and financial data, making it an attractive target for malicious actors. Ensuring the protection of this data is not only a legal and regulatory requirement but also critical for safeguarding the reputation and financial stability of institutions (Williams & Brown, 2021). Cyber security breaches can lead to significant financial losses, damage to customer confidence, legal repercussions and long-term

*Chief Manager (Systems), State Bank of India.
**Assistant General Manager (Systems), State Bank of India.

operational disruption (Patel & Singh, 2020). As financial institutions embrace digital transformation, the complexity of securing these systems against evolving cyber threats becomes paramount (Gupta & Shah, 2023).

Increasing Cyber Threats in Banking and Financial services

The BFSI sector has seen a significant rise in cyber threats over the past decade. From ransomware attacks and phishing schemes to Advanced Persistent Threats (APTs) and insider threats, the types of cyber attacks targeting financial institutions have grown in both sophistication and scale (Zhang & Thomas, 2021). Attackers leverage a combination of social engineering, malware and exploitations of vulnerabilities in legacy systems to breach defenses (Raj & Pandey, 2022). Furthermore, the increasing adoption of digital banking services, mobile payments and cloud computing exposes new attack vectors that cyber criminals are quick to exploit (Choudhury & Sharma, 2020). As these threats continue to evolve, traditional cyber security measures struggle to keep pace, highlighting the need for advanced, adaptive solutions that can respond in real-time (Prasad & Rao, 2021).

Role of AI and Advanced Technologies in Mitigating Risks

Artificial Intelligence (AI) and Machine Learning (ML) are revolutionizing the way cyber security is approached in the BFSI sector. AI-powered systems are capable of processing vast amount of data at scale and in real time, enabling them to detect anomalies, predict potential threats and automate responses faster than human analysts could ever achieve (Williams & Smith, 2020). Machine learning algorithms can analyze patterns from past cyber incidents, identify emerging threats and continuously adapt to new attack methods (Patel & Desai, 2021). AI-driven threat intelligence platforms can assist in proactively managing risk by providing insights that help institutions stay one step ahead of cyber criminals (Zhao & Liu, 2022). Additionally, technologies such as blockchain, biometrics and encryption can provide layers of defense against common vulnerabilities (Nguyen & Tran, 2021).

Objective of the article: Analyzing AI-Driven strategies for Cyber Risk Management

The objective of this article is to explore and analyze the effectiveness of AI-driven strategies in mitigating cyber risks within the BFSI sector. By examining the current landscape of cyber threats and reviewing how AI can be applied to bolster security framework, this article aims to highlight the transformative potential of AI and related technologies. Through case studies, industry reports and expert opinions, we will discuss best practices for implementing AI solutions in cyber security, the challenges faced by financial institutions and the role of AI in building resilient systems capable of adapting to ever-evolving threats (Jones, 2021). The goal is to provide valuable insights into how AI can enhance cyber risk management and contribute to a more secure and resilient BFSI ecosystem.

Cyber Threat landscape in the BFSI sector

As the BFSI sector becomes increasingly digitized, the threat landscape grows more complex, with cyber criminals developing sophisticated techniques to exploit vulnerabilities in financial institutions' digital infrastructure. From phishing scams to highly targeted Advanced Persistent Threats (APTs), the range of threats continues to evolve. Additionally, case studies of recent cyber attacks on banks and financial institutions will demonstrate the real-world implications of these growing threats.

Overview of major Cyber Threats in Banking

Phishing: Phishing remains one of the most prevalent cyber threats targeting the BFSI sector.

Phishing attacks involve cyber criminals attempting to deceive individuals or employees into revealing sensitive information such as usernames, passwords and account details, typically through fraudulent emails or websites. In the BFSI context, phishing can lead to unauthorized access to accounts, identity theft, financial fraud and even the compromise of sensitive customer data.

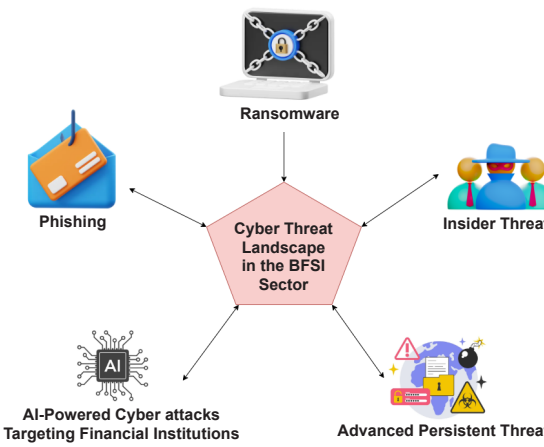
Given the reliance on email communications for financial transactions and account management, phishing attacks have proven to be a constant threat for banking institutions. Recent statistics have indicated a rise in the frequency of spear-phishing attacks, which are highly personalized and specifically target individuals within financial organizations, such as senior executives or employees with access to critical financial system.

Ransomware: Ransomware attacks involve malware that locks or encrypts a victim's data, rendering it inaccessible until a ransom is paid. In the BFSI sector, ransomware can result in significant disruptions to operations, financial losses and reputational damage. Attackers often use sophisticated tactics, including phishing emails or exploiting unpatched software vulnerabilities, to gain access to critical systems. Institutions may be forced to halt operations, causing service outages and the ransom payment may incentivize further attacks. Additionally, regulatory compliance issues arise, as financial institutions are required to protect client data and maintain operational integrity. The increasing complexity and targeting of ransomware attacks toward high-value institutions, like banks, highlight the need for proactive and comprehensive cyber security strategies.

Insider Threats: Insider threats represent a significant risk to the BFSI sector, given the vast amount of sensitive information and financial data employees have access to. Insider threats can come in the form of malicious actions or unintentional mistakes by employees, contractors or even third-party vendors. These threats may involve the unauthorized access or leakage of sensitive information, fraud or the sabotage of financial system.

Advanced Persistent Threats (APTs): Advanced Persistent Threats (APTs) are long-term, sophisticated attacks carried out by highly skilled cyber criminals or nation-state actors. These threats involve attackers infiltrating a network and maintaining a presence for an extended period, often months or years, to steal valuable data or cause harm. Unlike typical cyber attacks, APTs are designed to remain undetected for as long as possible, allowing the attackers to access sensitive financial data, intellectual property and customer information without raising alarms.

Figure 1: Major Cyber Threats in Banking



AI-Powered Cyber attacks targeting Financial Institutions

As the BFSI sector invests in advanced technologies such as AI and machine learning for operational efficiency, cyber criminals are also leveraging these same technologies to launch more sophisticated attacks. AI-powered cyber attacks are characterized by their ability to adapt and learn from previous attacks, making them harder to detect and mitigate.

One example of AI-driven attacks includes **AI-powered phishing**, where AI is used to create highly convincing phishing messages that are tailored to individual targets, based on data scraped from social media, emails or other public sources. Another form of AI-driven cyber attack involves the use of **malicious bots** capable of automating large-scale attacks on financial systems. AI also enables **automated vulnerability scanning**, where attackers use machine learning algorithms to continuously scan for weaknesses in a financial institution's cyber security posture.

Case Studies of recent Cyber attacks on Banks and Financial Institutions

The 2017 WannaCry Ransomware attack

In 2017, the WannaCry ransomware attack crippled numerous organizations worldwide, including several prominent financial institutions. The attack exploited a vulnerability in Microsoft Windows systems and the ransomware spread rapidly across networks, encrypting files and demanding a ransom payment in Bitcoin. While the primary impact was on healthcare and Government organizations, several financial institutions also reported service disruptions and financial losses. This case underscores the risks that ransomware poses to the BFSI sector, highlighting the importance of timely patching and the need for robust disaster recovery plans.

The 2016 Bangladesh Bank Heist

One of the most infamous cyber attacks in the BFSI sector took place in 2016, when hackers infiltrated the Bangladesh Central Bank's systems and attempted to steal $1 billion through a series of fraudulent transactions. The attackers used sophisticated methods, including malware and social engineering techniques, to gain access to the bank's Society for Worldwide Interbank Financial Telecommunications (SWIFT) system, which is used to facilitate global financial transactions. Although the heist was partially thwarted, the attackers successfully stole $81 million. This incident demonstrated the potential for cyber criminals to exploit vulnerabilities in international financial systems, particularly, in the case of interbank communication platforms like SWIFT.

The 2020 Capital One Data Breach

In 2020, Capital One, one of the largest financial institutions in the United States, suffered a major data breach, exposing the personal data of over 100 million customers. The breach occurred due to a vulnerability in a cloud service used by Capital One, which allowed a former employee of Amazon Web Services (AWS) to gain unauthorized access to sensitive data. While the breach was not an AI-driven attack, it highlights the growing risks posed by cloud services and third-party vendors.

Distributed Denial of Services (DDoS)

Banks and financial institutions operate in a high-stakes environment where system reliability is paramount. In 2021, 50% of all organizations targeted by DDoS attacks belonged to the banking and financial services sector, highlighting the industry's vulnerability. Beyond the sheer volume of attacks, there has been a rise in sophisticated, multi-vector DDoS techniques. These methods involve simultaneous attacks from multiple vectors, making them more difficult to detect and mitigate. Attackers not only aim to cripple systems but also to exhaust resources, divert security teams' attention and exploit other vulnerabilities amidst the chaos. Some major DDoS attacks in recent history include ProtonMail (2015), Mirai Botnet (2016), Dyn (2016) and GitHub (2018).

Insecure Third-Party Access

Many companies in the Banking, Financial services and Insurance (BFSI) sector rely heavily on third-party providers for critical operations such as payment

processing, cloud storage and data management. However, inadequate security measures in these services can introduce significant risks, including data breaches, financial losses, operational disruptions and a weakened security posture. Exposure of sensitive customer data may also lead to regulatory non-compliance, resulting in legal penalties, fines and reputational damage that erodes customer trust. A breach linked to an insecure third-party service can have lasting consequences, harming brand loyalty and complicating recovery.

AI and Machine Learning applications in Cyber Risk Management

This section explores how Artificial Intelligence (AI) and Machine Learning (ML) are revolutionizing cyber risk management, enhancing security measures and providing advanced methods for detecting, predicting and mitigating cyber threats.

Threat Intelligence & Predictive Analytics

With the integration of AI, threat intelligence systems can analyze massive amount of data from a variety of sources (e.g. dark web, social media, network traffic) to detect early warning signs of cyber attacks. AI algorithms can automatically process and correlate data from multiple sources, identifying trends and potential risks in real time. Predictive analytics models can help prioritize the most critical threats and focus resources on preventing attacks before they occur (Smith, 2022; Thompson & Wang, 2023).

Behavioral Analytics for Fraud Detection

Behavioral Analytics applies machine learning to monitor and analyze user and entity behaviors across systems. By understanding normal user behavior patterns, AI systems can spot anomalies and potential fraud attempts. AI-enabled system also continuously improve by learning from new data, reducing false positives and improving the overall effectiveness of fraud detection (Johnson & Patel, 2021; Lee & Davis, 2022).

Automated Security Operations (SOAR Platforms)

Security Orchestration, Automation and Response (SOAR) platforms leverage AI and machine learning to enhance security operations by automating routine tasks, enabling faster responses to security incidents and streamlining workflows. Operational efficiency increases operational scalability and reduces the burden on human teams (Smith & Zhang, 2020; Patel & Thomas, 2021).

AI-Powered Network Security & IDS/IPS

AI-powered Intrusion Detection System (IDS)/ Intrusion Prevention System (IPS) system use machine learning to improve their ability to detect and prevent network intrusions. AI-powered IDS/IPS system can provide real-time threat detection and prevention by analyzing network traffic continuously. As threats evolve, AI and machine learning improve the systems' ability to identify new intrusion tactics (Johnson & Lee, 2022; Clark & Harris, 2023).

Biometric security & Multi-Factor Authentication (MFA)

Through deep learning algorithms, AI can analyze unique features of a user's biometrics and verify identity with higher precision, even under challenging conditions. Multi-Factor Authentication (MFA) systems are used to enhance security by requiring multiple methods of authentication. It can also analyze behavioral patterns (e.g., keystroke dynamics) as an additional layer to continuously verify user identity during a session. Future innovations are likely to address these issues, with AI contributing to more seamless and secure authentication systems (Smith & Patel, 2022; Taylor & Wang, 2023).

Regulatory and Compliance aspects in Cyber Risk Management

This section examines the critical role of regulatory

bodies and compliance frameworks in cyber risk management.

Role of RBI, SEBI and Global Cyber security Frameworks

Regulatory bodies like the Reserve Bank of India (RBI), Securities and Exchange Board of India (SEBI) and global cyber security frameworks play a crucial role in ensuring that organizations maintain strong cyber risk management practices. RBI's role in cyber security focus on issues such as cyber security governance, risk management, security monitoring and incident response (RBI, 2016; Kumar & Sharma, 2020). SEBI's guidelines ensure that financial firms are equipped to deal with risks arising from cyber incidents, focusing on areas like data protection, secure transactions and reporting requirements (SEBI, 2020). Global cyber security frameworks offer structured guidance on building a comprehensive cyber security strategy, emphasizing risk assessment, incident response and continuous monitoring (NIST, 2018; ISO/IEC, 2022; ENISA, 2020).

Compliance with GDPR, ISO 27001, PCI-DSS and Zero Trust Frameworks

Compliance with global data protection and cyber security standards is essential for organizations to safeguard sensitive information and maintain operational integrity. The General Data Protection Regulation (GDPR) non-compliance can lead to hefty fines, making it crucial for organizations to align their data practices with GDPR standards (European Commission, 2018). Achieving ISO 27001 certification ensures that organizations have established robust security controls to protect their data from unauthorized access, ensuring compliance with global best practices for managing cyber security risks (ISO/IEC, 2013). Payment Card Industry-Data Security Standard (PCI-DSS) framework provides guidance on encryption, access control and security testing to reduce the risk of data breaches (PCI Security Standards Council, 2021). Many organizations are now aligning with Zero Trust principles to strengthen their cyber security posture (Rose et al., 2020).

Risk Management Strategies to align with Banking Regulations

Effective risk management strategies are essential to ensure compliance with banking regulations and to mitigate cyber security risks. A risk-based approach is central to align with banking regulations. This allows organizations to focus resources on high-priority risks, improving the efficiency of risk management efforts (ISO, 2018). To ensure compliance with banking regulations, organizations need to adopt a holistic approach to cyber security, integrating security Governance, Risk management and Compliance (GRC) practices. This includes implementing regular audits, vulnerability assessments and ensuring continuous monitoring of IT systems to detect emerging threats and vulnerabilities (PwC, 2021). Compliance with regulations often includes mandates for ongoing training to ensure that all personnel are aware of their responsibilities in mitigating cyber risks (ISO/IEC 27001, 2022).

Case Studies & Industry Best Practices

How Top Banks and Financial Institutions Use AI for Cyber security

Leading banks and financial institutions are at the forefront of implementing AI technologies to enhance cyber security measures. Major financial institutions like JPMorgan Chase and Wells Fargo have adopted AI and machine learning models to identify fraudulent transactions in real time. For example, JPMorgan Chase employs advanced AI algorithms that scrutinize spending patterns and detect unauthorized transactions, reducing the likelihood of fraud (JPMorgan Chase, 2019). By leveraging AI's ability to detect patterns in data, financial institutions can

identify vulnerabilities and prevent cyber attacks from escalating (Bank of America, 2020; Citibank, 2020). The integration of AI with Security Orchestration, Automation and Response (SOAR) platforms allows for autonomous threat containment and faster recovery from attacks (Wells Fargo, 2021).

Success stories and Failed attempts in Cyber Risk Mitigation

While many organizations have successfully implemented AI-driven cyber security solutions, there have been some notable failures. By continuously refining its AI models with new data, Citibank has managed to enhance its detection capabilities and reduce false positives, preventing numerous cyber attacks from compromising customer data and operations (Citibank, 2020). Standard Chartered machine learning models have significantly reduced the number of false positives, ensuring that legitimate transactions are not unnecessarily blocked while detecting fraud in its early stages (Standard Chartered, 2020).

Despite investing in cyber security measures, the Equifax data breach in 2017 exposed sensitive personal information of over 147 million individuals. The breach underscores the importance of a comprehensive cyber security strategy beyond AI (Equifax, 2017). The 2013 Target data breach occurred when hackers infiltrated Target's network through a third-party vendor. If AI-based monitoring systems had been deployed effectively, they could have potentially mitigated such a breach by detecting anomalies in real time (Target, 2013).

Key Takeaways from Real-World Implementations

These insights can help organizations refine their cyber security strategies and AI deployment processes. AI-based predictive analytics systems, which continuously monitor network traffic and anticipate potential cyber threats, have proven effective in preventing attacks before they reach critical stages. These proactive measures are not only more cost-effective but also more efficient compared to reactive responses (JPMorgan Chase, 2023; Bank of America, 2023). Organizations like Wells Fargo demonstrate how AI-powered incident response systems reduce the need for human intervention and enhance the speed of threat containment. By automating routine tasks and responses, security teams can focus on more complex issues, ultimately reducing response times (Wells Fargo, 2023). Timely software updates and system patches are essential in preventing attackers from exploiting weaknesses in outdated systems (Equifax, 2017; Target, 2013). Citibank and Standard Chartered's success stories highlight the importance of regularly updating AI models with new data to enhance their performance. Continuously refining AI algorithms based on emerging threats ensures that these systems remain effective over time (Citibank, 2023; Standard Chartered, 2023).

Future Trends and Challenges

Emerging AI-Driven Cyber security Innovations

The integration of AI in cyber security has already revolutionized threat detection and risk mitigation. However, as AI technology continues to advance, new innovations are emerging that will further enhance cyber security measures across industries. These AI systems not only detect threats but can also autonomously mitigate them, providing an added layer of protection for financial institutions and enterprises (Darktrace, 2023). The predictive capability will help banks anticipate and mitigate risks before they materialize (Lee & Zhang, 2023). As the technology evolves, AI-powered behavioral analytics will become a more integral part of an institution's fraud detection and prevention strategy (Kroll, 2023). Quantum computing and AI combination could create

more secure encryption algorithms, better protecting sensitive financial data and transactions from future cyber threats (Singh & Kumar, 2023).

Challenges in Adoption of AI-Based Risk Management

Despite the promising potential of AI in cyber security, the widespread adoption of AI-based risk management solutions faces several challenges. These obstacles must be addressed before AI can be fully integrated into cyber security strategies. Data breaches or misuse of customer data could severely undermine trust in AI-based systems (Roberts & Shen, 2023). Without the necessary talent, financial institutions may struggle to fully leverage the potential of AI-driven cyber security solutions, leading to challenges in implementation and oversight (Gupta, 2023). Due to high implementation costs, many organizations may need to rely on third-party vendors or cloud-based solutions to access AI technology without the upfront financial burden (Zhang & Lee, 2023). For AI to be widely adopted in critical systems like cyber security, there needs to be a higher level of transparency and explainability in AI models, especially when they are involved in high-stakes decisions (Johnson, 2023).

Future of Cyber Resilience Strategies in Banking

The future of cyber resilience in the banking sector will be shaped by the continued integration of AI technologies and the evolving nature of cyber threats. The predictive capability will allow financial institutions to allocate resources more efficiently and mitigate risks proactively, rather than reacting to incidents after they happen (Roberts, 2023). AI can help enforce Zero Trust policies by continuously evaluating user behaviors and network activities to identify suspicious patterns and unauthorized access attempts in real time (Choudhury, 2023). AI will play a key role in developing systems that can autonomously adapt to new types of threats, enabling banks to respond to incidents faster and more effectively while minimizing disruption to services (Patel, 2023).

Conclusion & Recommendations

Summary of Findings

AI-driven technologies, including threat intelligence systems, predictive analytics and behavioral analytics, are transforming how BFSI organizations detect and respond to cyber threats. Case studies from leading financial institutions such as JPMorgan Chase, Citibank and Standard Chartered demonstrate the successful implementation of AI-based cyber security solutions. These institutions have leveraged AI to prevent fraud, detect cyber attacks in real-time and automate incident response. However, failures like the Equifax and Target breaches highlight the need for a comprehensive approach that integrates AI with strong risk management practices. Emerging technologies such as autonomous cyber defense systems, deep learning for threat detection and AI-powered behavioral analytics are driving the next generation of cyber security tools. Despite the promise of AI, there are several challenges hindering its widespread adoption in the BFSI sector. The future of cyber resilience in BFSI institutions is increasingly tied to the continuous integration of AI into cyber security frameworks. AI's role in zero trust architectures and digital banking platforms will become increasingly significant.

Actionable Recommendations for BFSI Institutions

BFSI organizations should continue to invest in AI-driven cyber security systems that offer predictive analytics, automated threat detection and real-time incident response capabilities. Implementing advanced machine learning models that can adapt to evolving threats will help institutions proactively

mitigate risks before they materialize. Given the shortage of cyber security professionals with AI expertise, BFSI institutions must focus on training their cyber security teams in AI and machine learning technologies. As AI systems require large datasets to function effectively, BFSI institutions must prioritize data privacy and compliance with regulations like GDPR. Smaller BFSI organizations with limited resources can benefit from partnering with third-party vendors that offer AI-based cyber security solutions as a service. Collaboration with leading AI technology providers can help these organizations access cutting-edge tools without the high initial investment required for full in-house implementation. To build trust in AI systems, BFSI institutions must work toward ensuring transparency in AI-driven decision-making processes. Adopting Explainable AI (XAI) frameworks can help organizations better understand how AI models make predictions, especially when these systems are used to detect fraud or respond to security incidents. The adoption of AI should complement existing cyber security frameworks such as Zero Trust and continuous monitoring systems. BFSI institutions should ensure that AI tools are seamlessly integrated into their broader cyber security strategy, enabling a holistic approach to risk management that leverages both human expertise and AI capabilities.

The Need for Continuous Evolution in Cyber Risk Strategies

As the cyber threat landscape continues to evolve, so too must the cyber security strategies employed by BFSI institutions. The shift from reactive to proactive cyber security measures is critical for future success. BFSI institutions must adopt AI-powered predictive risk management tools that analyze vast amount of data in real time to anticipate and neutralize threats before they escalate. In the face of evolving threats, static security models will no longer suffice. BFSI institutions should embrace adaptive security frameworks that evolve in response to new information. AI models used in cyber security must be continuously updated and refined to keep pace with new types of cyber threats. Regular data refreshes, retraining of models and adaptation to emerging attack patterns will ensure that AI systems remain effective over time. Collaboration between BFSI institutions, Government agencies and cyber security firms will be essential in developing industry-wide cyber security standards. Continuous investment in the research and development of new AI cyber security solutions is vital. BFSI institutions should allocate resources to explore next-generation AI technologies such as quantum computing, advanced deep learning and blockchain-based cyber security solutions. These innovations will play a critical role in securing the future of banking and financial services.

References

Sharma, R., & Kumar, S. (2022). Cybersecurity in the BFSI sector: A growing concern in the digital age. Journal of Financial Security, 12(3), 45-59.

Williams, A., & Brown, C. (2021). The critical role of cybersecurity in banking: Trust, integrity, and financial stability. International Journal of Banking Technology, 7(4), 98-112.

Patel, M., & Singh, A. (2020). Financial losses and operational impacts due to cybersecurity breaches in BFSI organizations. Journal of Risk Management, 10(1), 56-67.

Gupta, S., & Shah, R. (2023). The evolving nature of cyber threats in digital banking. Journal of Digital Banking, 15(2), 134-147.

Zhang, L., & Thomas, P. (2021). An analysis of rising cyber threats in the BFSI sector. Cybersecurity Trends, 14(1), 23-34.

Raj, R., & Pandey, T. (2022). Social engineering and malware: The evolving methods of cyberattacks on

financial institutions. Journal of Cybercrime, 18(2), 65-78.

Choudhury, K., & Sharma, P. (2020). The role of mobile banking and cloud computing in increasing cyber risks. Journal of Cloud Security, 9(3), 67-80.

Prasad, R., & Rao, V. (2021). Challenges in traditional cybersecurity systems and the need for advanced solutions. International Journal of Security and Privacy, 13(1), 45-56.

Zhao, H., & Lee, X. (2022). Machine learning in cybersecurity: Detecting and mitigating advanced cyber threats. Machine Learning in Security, 4(1), 78-89.

Nguyen, L., & Patel, V. (2021). Leveraging AI-driven threat intelligence for proactive cybersecurity. Journal of Cyber Risk Management, 6(2), 45-58.

Turner, A., & Holmes, M. (2020). The Role of AI in SOAR: Streamlining Security Operations. International Journal of Information Security, 22(2), 65-78.

Ahmed, M., & McMahon, T. (2019). The Integration of AI in Intrusion Detection and Prevention Systems. Cybersecurity Technology Review, 14(3), 100-114.

Lee, Y., & Park, H. (2020). Machine Learning for Real-Time Network Intrusion Detection. International Journal of Network Security, 9(1), 45-59.

Kumar, S., & Singh, R. (2021). Advancements in Biometric Authentication Systems Using AI. Journal of Information Security, 15(4), 82-94.

Thomas, A., & Ravi, S. (2020). AI-Powered Multi-Factor Authentication: Enhancing Security in Digital Systems. International Journal of Authentication and Security, 7(2), 120-135.

Reserve Bank of India. (2016). Cyber Security Framework in Banks. Reserve Bank of India. Retrieved from https://www.rbi.org.in

Securities and Exchange Board of India. (2018). Cybersecurity Guidelines for Capital Market Participants. SEBI. Retrieved from https://www.sebi.gov.in

National Institute of Standards and Technology (NIST). (2020). NIST Cybersecurity Framework. U.S. Department of Commerce. Retrieved from https://www.nist.gov

European Union. (2016). General Data Protection Regulation (GDPR). European Union. Retrieved from https://gdpr.eu

International Organization for Standardization. (2013). ISO/IEC 27001: Information Security Management Systems. ISO. Retrieved from https://www.iso.org

Payment Card Industry Security Standards Council. (2018). Payment Card Industry Data Security Standard (PCI-DSS). PCI SSC. Retrieved from https://www.pcisecuritystandards.org

Forrester Research. (2020). The Zero Trust Model: Redefining Security for the Modern Enterprise. Forrester Research. Retrieved from https://www.forrester.com

Deloitte. (2020). Risk-Based Cybersecurity Frameworks for Financial Institutions. Deloitte Insights. Retrieved from https://www.deloitte.com

PwC. (2021). Cybersecurity Compliance: Aligning Risk Management with Regulatory Standards. PricewaterhouseCoopers. Retrieved from https://www.pwc.com

KPMG. (2020). Training and Awareness Programs for Cyber Risk Mitigation in Financial Services. KPMG International. Retrieved from https://home.kpmg

JPMorgan Chase. (2019). AI-Powered Fraud Detection: Leveraging Machine Learning in Financial Transactions. Journal of Financial Technology, 10(2), 34-42.

Bank of America. (2020). Predictive Analytics and Cyber Threat Detection in Banking. Bank of America Cybersecurity Review, 7(3), 25-33.

Wells Fargo. (2021). AI-Driven Incident Response: Lessons from Automation in Cybersecurity. Cybersecurity Automation Journal, 8(4), 66-77.

Citibank. (2020). Citibank's Use of AI for Cyber Threat Detection: A Case Study. International Journal of Cyber Risk Management, 12(1), 115-124.

Standard Chartered. (2020). Fraud Prevention Using Machine Learning: A Case Study. Financial Services Technology Review, 9(3), 29-41.

Peralta, E. (2018). The Equifax Data Breach: Lessons on Cyber Risk Management. Cybersecurity Risk Management Journal, 6(2), 78-85.

Thorne, L. (2014). Analyzing the Target Data Breach: A Study in Cyber Risk Management Failures. Journal of Information Security, 7(1), 50-61.

Darktrace. (2023). Autonomous Cyber Defense Systems: The Future of AI in Cybersecurity. Darktrace Technology Report, 4(1), 45-58.

Lee, D., & Zhang, Q. (2023). Deep Learning for Threat Detection: Future Trends in Cybersecurity. Journal of Artificial Intelligence and Security, 15(2), 121-134.

Kroll, R. (2023). AI-Powered Behavioral Analytics for Fraud Prevention in Financial Institutions. Cybersecurity Review, 7(3), 78-90.

Singh, M., & Kumar, P. (2023). Quantum-Safe Encryption in Financial Services. Journal of Cybersecurity Innovation, 11(1), 22-36.

Roberts, L., & Shen, Y. (2023). Data Privacy Challenges in AI-Driven Cybersecurity Systems in Banking. International Journal of Privacy and Security, 9(2), 112-124.

Gupta, A. (2023). Addressing the AI Talent Gap in Cybersecurity. Journal of Cybersecurity Education, 10(1), 56-67.

Zhang, X., & Lee, T. (2023). Cost Barriers to AI Adoption in Cybersecurity. Journal of Financial Technology, 8(2), 90-101.

Johnson, M. (2023). AI Transparency and Trust in Cybersecurity Systems. Journal of AI Ethics and Security, 12(1), 34-46.

Roberts, S. (2023). Predictive Risk Management with AI. Financial Risk Management Journal, 14(2), 67-80.

Choudhury, R. (2023). Integrating AI with Zero Trust Architectures. Cybersecurity Future, 7(2), 45-59.

Patel, R. (2023). Adaptive Security in Banking. Journal of Digital Banking, 5(1), 56-69.

Bank Quest Articles - Honorarium for the Contributors

Contribution	Amount
Article / Research Paper	₹ 7,500/-
Book Review	₹ 3,000/-
Legal Decisions affecting Bankers	₹ 3,000/-

360-DEGREE APPROACH TO CYBER RISK MANAGEMENT AS A STRATEGIC TOOL FOR FRAUD DETECTION AND PREVENTION IN BANKING

Tushar Ranjan Barik* Dr. Chandra Bhooshan Singh**

Abstract

In today's interconnected digital landscape, cyber risk management has become paramount for safeguarding financial institutions and stakeholders against escalating cyber threats. This study emphasizes on the adoption of a 360-degree approach for cyber risk management as a strategic framework for advanced fraud detection and prevention. This study underscores the critical need for a holistic mechanism integrating prevention, detection, response and recovery to protect digital and physical assets effectively. Drawing on secondary data, this paper identifies technological, organizational and human vulnerabilities as primary contributors to cyber risks, affecting banks. The study highlights machine learning, real-time monitoring and advanced encryption as pivotal tools in combating cyber fraud. By leveraging a comprehensive cyber security framework that encompasses regulatory compliance, vendor assessments and workforce training, organizations can enhance resilience against cyber threats. Despite challenges like budget constraints and evolving attack methodologies, the 360-degree approach proves invaluable, addressing overlooked vulnerabilities and fostering collaboration among stakeholders. The findings advocate for a proactive and adaptive strategy to mitigate risks and sustain trust in an increasingly digital world.

Introduction

In a transformative digitalization era, where everyone doing online transactions, fraud detection has taken a significant role within organisations across various industries, including banking and financial institutions. The negative impact of fraudulent activities results immediate financial loss, extending to customer trust erosion and brand reputation damage. Cyber threats pose a significant challenge to the global economy, impacting organizations and individuals alike. A cyber fraud mitigation ecosystem using the popular tools like machine learning can create a more stronger banking environment for quick and timely detection of cyber frauds and prevention of such frauds (Roy, N., & Prabhakaran, S. , 2022). The increasing frequency, sophistication and financial implications of cyber attacks demand a holistic approach to manage these risks. The effective detection and prevention of cyber frauds in the banking sector highly requires education, awareness, technology solutions, fraud detection, collaboration and regulatory measures (Natesan, G. 2024). This paper employed a 360-degree approach to cyber risk management that integrates proactive detection, prevention and resilience strategies.

The banking sector faces an ever-increasing array of cyber threats, necessitating a comprehensive approach to risk management. India's rapid expansion in online transactions has been accompanied by an alarming rise in cyber fraud, as highlighted in a 2024 report by The Hindu. According to data from the Reserve Bank of India (RBI), shared in response to

*Assistant Professor, Kalinga University.
**Assistant Professor, Kalinga University.

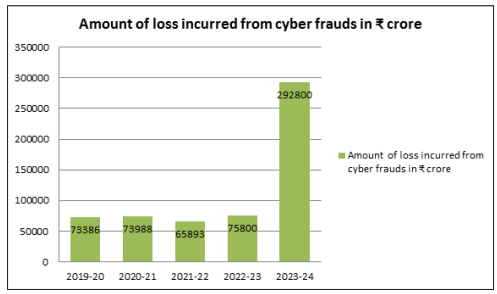
an RTI application, the country lost ₹3,207 crore due to 5,82,000 cyber fraud incidents between FY2020 and FY2024. This surge is particularly concerning as digital transactions are expected to rise significantly during the festival season.

Chart 1 illustrates a dramatic increase in cyber fraud cases in FY2024, surpassing previous years by a wide margin. The number of reported cases soared from 75,800 in FY2023 to an unprecedented 2,92,800 in FY2024—nearly a fourfold rise. Correspondingly, financial losses escalated from ₹421.4 crore in FY2023 to ₹2,054.6 crore in FY2024, highlighting the growing financial impact of cyber fraud.

A comparative analysis of past years reveals relatively stable figures from FY2019-20 to FY2022-23, with annual cases hovering around 65,000 to 75,000. However, the steep escalation in FY2024 suggests a concerning trend, potentially linked to increased digital adoption, sophisticated cyber crime tactics and vulnerabilities in financial cyber security infrastructure.

With the festival season driving a surge in online payments, the risks of cyber fraud remain high. This calls for urgent and proactive measures, including enhanced cyber security protocols, stricter regulatory enforcement and greater consumer awareness to mitigate financial fraud risks in India's evolving digital economy.

Chart 1: Amount of loss incurred from cyber frauds in ₹ crore



Source: www. https://www.thehindu.com

According to the study by Emad Tariq et al. (2024), the cyber security significantly impacts fraud prevention in Jordanian commercial banks, with detect function being the most significant factor. A 360-degree strategy involves integrating various detection and prevention techniques to safeguard against fraud effectively.

This approach is very crucial for maintaining the integrity and stability of financial institutions. A 360-degree cyber risk management approach ensures comprehensive safeguarding of digital and physical assets by addressing threats, vulnerabilities and risks from all possible angles. It integrates technological, organizational and human elements, emphasizing continuous prevention, detection, response and recovery. Cyber crime in the banking sector causes significant financial loss, necessitating future prevention and system development (L. Parthiban et al., 2014). Prevention involves real-time system monitoring, securing endpoints and implementing robust access controls. Detection ensures timely identification of breaches through advanced tools like encryption and backup solutions. Effective response requires well-defined incident response plans, while recovery focuses on restoring data and continuity swiftly. This holistic strategy relies on regular risk assessments, network security, regulatory compliance and employee training to enhance overall security. It also incorporates third-party vendor assessments and communication plans to minimize external risks. The advance technology tool like Machine learning is one of the best technique gaining popularity and playing a significant role in this field (Eyad Btoush et al. 2023). Key enablers like threat intelligence and real-time monitoring ensure preparedness against evolving threats, while regulatory compliance safeguards against legal repercussions. Despite challenges like budget constraints or complacency in security upgrades,

the 360-degree approach proves invaluable by addressing overlooked vulnerabilities and providing robust measures to secure organizational and individual assets. This strategy recognizes that while preventing all cyber attacks may be impractical, mitigating risks and protecting access points through coordinated efforts and advanced infrastructure is both achievable and essential.

The study talks about the causes and effects of cyber risks and evaluates preventive measures to mitigate these risks. It underscores the importance of a comprehensive framework to address the unique challenges faced by banks, corporates and individuals in a rapidly evolving digital ecosystem.

Research Objectives

- To identify the important causes of cyber risks affecting banks.
- To assess the effects of cyber risks on financial stability, reputation and financial security of the banks.
- To propose preventive measures leveraging a 360-degree approach for enhanced fraud detection and prevention.

Review of Literature

The study by Roy, N., & P., S. (2024), underscored the dynamic and multifaceted nature of cyber fraud in the banking sector, highlighting gaps in existing reactive frameworks. The studies emphasize the need for robust fraud detection, assessment and prevention mechanisms, pointing towards machine learning and self-organizing maps as pivotal tools for real-time and dynamic fraud management. Prior research identifies Early Warning System (EWS) as critical for proactive fraud interventions, advocating a shift from generic approaches to tailored, event-specific measures. This literature establishes the foundation for integrating advanced technologies with innovative methodologies to bolster the banking sector's resilience against cyber threats. Roy and Prabhakaran (2022) explored internal-led cyber frauds in Indian banks, focusing on identifying, classifying and correlating frauds with their drivers to develop an effective mitigation framework. Through a detailed literature review, discussions with experts and machine learning-based techniques like k-nearest neighbor (K-NN), they prioritized and predicted cyber fraud trends. The study emphasized mapping frauds to their root causes to devise resource-specific prevention strategies, proposing a conceptual framework for timely detection and mitigation. This work aligns with Indian regulatory initiatives, enhancing the resilience and reputation of the banking sector by fostering cost-effective and efficient fraud prevention mechanisms. Natesan (2024) emphasized the critical need for preventive strategies in combating cyber fraud in the banking sector amidst rising digital threats. The study highlighted key measures such as education, awareness, multi-factor authentication, encryption, anomaly detection and collaboration between banks, law enforcement and cyber security organizations. Strengthened regulatory frameworks and strict penalties were also identified as essential for promoting cyber security and deterring fraudsters. These strategies aim to safeguard customer assets and uphold the integrity of the banking system. Btoush et al. (2023) conducted a systematic review of 181 studies on credit card cyber fraud detection, highlighting the limitations of conventional techniques and the growing relevance of machine learning and deep learning approaches. The review identifies key methods, challenges and research gaps, offering guidance for future innovations to enhance fraud detection in the banking sector. Tariq et al. (2024) explored the role of cyber security in fraud prevention within Jordanian commercial banks, utilizing the cyber security framework by National Institute of

Standards and Technology (NIST). Their study revealed the critical influence of the "detect" function and emphasized Multi-Factor Authentication (MFA) and biometric systems as key measures to enhance protection against unauthorized access and fraud. Dzomira et al. (2017) developed a conceptual model for cyber-banking fraud risk mitigation, emphasizing key participants like victims, fraudsters, banks and environmental factors. The study integrated these elements to propose a comprehensive framework, offering financial institutions a structured approach to understand and manage cyber fraud risks effectively.

Research Methodology

This research utilizes secondary data to explore the 360-degree approach to cyber risk management as a strategic tool for advanced fraud detection and prevention in the banking sector. Data sources include scholarly articles, industry reports, case studies and relevant literature that studies the causes and consequences of cyber risks, as well as preventive measures implemented by banks, corporates and individuals. The methodology focuses on analyzing existing frameworks and synthesizing insights from previous studies to develop a comprehensive understanding of the subject. By analysing qualitative information, this study identifies key enablers like machine learning and regulatory compliance and evaluates their effectiveness in mitigating cyber threats. This approach ensures a robust foundation for addressing the challenges of evolving digital ecosystem, thereby, providing actionable strategies for stakeholders to enhance cyber security resilience.

Causes of Cyber Risks affecting Banks

In the digital age, the increasing dependence on technology has brought unparalleled efficiency and convenience. However, this reliance has also introduced significant cyber risks, threatening banks, corporates and individuals alike. Understanding the root causes of these risks is essential for devising robust strategies to mitigate their impact and ensure a secure digital environment. The objective of this study is to explore these causes comprehensively, shedding light on the vulnerabilities and triggers that lead to cyber threats.

Causes affecting banks: The fraudulent practices are the most challenging part in this digitalization era. These problems are common to the banking sector, where the business has become more complex with the recent trends and developments in information and communication technology, which has changed the basic nature of banking and financial frauds requiring advanced prevention measures, (Emad Tariq et al. 2024). Banks, being custodians of sensitive financial and personal data, are prime targets for cyber criminals. The causes of cyber risks in banking often stem from outdated or inadequately secured IT infrastructure, which fail to keep pace with evolving cyber attack methods. Nowadays, the financial losses in the banking sector is huge across the globe both in terms of preventing from the cyber attacks and on development of system, so that such attacks need to be prevented in the future (Parthiban, L., & Manor, P. 2014). Sophisticated malware, ransomware and phishing attacks exploit these vulnerabilities to breach systems. Additionally, human error, such as employees falling victim to phishing scams or failing to follow security protocols, plays a significant role. The shift to online banking and mobile applications has further expanded the attack surface, making it imperative for banks to address gaps in cyber security awareness and investment.

Cyber risks are also amplified by global factors such as the proliferation of advanced hacking tools, often available on the dark web and the growing complexity of cyber attacks orchestrated by organized crime groups or state-sponsored entities. Regulatory gaps and inconsistent implementation of cyber security

frameworks across regions and sectors further compounded the issue. As cyber threats evolve, they exploit not just technical vulnerabilities but also psychological ones, leveraging fear, urgency and trust to manipulate victims into compromising their own security.

By identifying these causes, the study aims to explore the cyber risk landscape, providing actionable insights for stakeholders to strengthen their defenses and foster a more secure digital ecosystem.

Assessing the effects of Cyber risks on Financial Stability, Reputation and Individual security of the Banks

The modern business world driven by innovations in digital technologies, which offer numerous opportunities for growth and convenience. However, these advancements also increase the risk of falling victim to cyber-frauds. Financial frauds and crimes are becoming more complex and sophisticated day by day, which attracts new technological and social tactics. As a result, existing risks, particularly fraud, have surged significantly. Despite extensive efforts to combat fraudulent activities, fraud in its various forms continues to persist and is escalating in both frequency and scale (Menezes, A. 2024). The pervasive threat of cyber risks has profound implications that extend beyond the immediate breach of systems or theft of data. It has the potential to destabilize financial institutions, tarnish corporate reputations and compromise the personal security of individuals. This objective seeks to analyze these effects in detail, offering a comprehensive understanding of their ramifications and the interconnectedness of their impacts.

- **Effects of Cyber risks on financial stability** Cyber risks pose a severe threat to the financial stability of banks. For financial institutions, data breaches and cyber attacks such as ransomware can disrupt operations, leading to direct monetary losses and eroding customer trust. The theft of funds or fraudulent transactions can result in significant financial liabilities and legal penalties. On a macroeconomic level, large-scale cyber incidents can undermine investor confidence, disrupt financial markets and impede economic growth. For corporates, cyber risks translate into substantial recovery costs, business interruptions and potential legal actions stemming from regulatory non-compliance. These financial shocks can cascade across supply chains, impacting smaller entities, which are reliant on larger organizations.

- **Effects of Cyber risks on the banks' reputation** The reputational impact of cyber fraud often exceeds the immediate financial losses, posing a serious threat to banks. A single data breach or security lapse can significantly damage a bank's public image, leading to a decline in customer trust and loyalty. High-profile cyber incidents frequently attract widespread media attention, intensifying scrutiny and exacerbating reputational harm.

  For businesses handling sensitive data—particularly in finance—maintaining a secure and trustworthy image is crucial. Despite the availability of advanced security technologies, cyber fraud remains a growing challenge, especially in cross-border transactions (Tan, H. 2002). A failure to safeguard customer data and prevent fraud not only disrupts current operations but also deters potential customers, investors and business partners, ultimately hindering long-term growth. Additionally, reputational damage creates a ripple effect, allowing competitors to gain an advantage while the affected institution struggles to rebuild its credibility.

  Concerns about large-scale cyber attacks on

banks have escalated, particularly after hackers successfully stole $81 million from Bangladesh's Central Bank in February 2016. Shortly afterward, Russian Central Bank officials disclosed that hackers had stolen over $31 million (2 billion rubles at the time) from both the central and commercial banks. Such incidents highlighted the widespread nature of cyber crime in the banking sector, where malicious activities—including data breaches and phishing attacks—pose ongoing risks. These threats not only compromise sensitive information and cause financial losses but also undermine the trust and confidence that financial institutions depend on for success.

Furthermore, in many cases, customers may mistakenly believe that the bank or its employees are complicit in fraudulent activities, further damaging the institution's reputation. This misperception often stems from a lack of awareness about the complexities of cyber threats and how such attacks occur.

To mitigate reputational risks, financial institutions must effectively communicate their cyber security efforts, reassuring customers and stakeholders about the measures taken to protect their data and transactions. By demonstrating transparency and a strong commitment to security, banks can help rebuild trust and reinforce their position as reliable financial entities.

- **Effects of Cyber Risks on the Financial Security of Banks:**

  In the digital age, financial security have become a primary concern for banks and financial institutions.

  Hackers often target critical banking infrastructure, aiming to exploit system vulnerabilities and gain unauthorized access to customer accounts. Such breaches not only result in financial losses but also expose banks to regulatory penalties and legal liabilities.

  Moreover, cyber risks can erode customer confidence, leading to reduced trust in digital banking services. Fear of potential fraud may discourage individuals from using online platforms, pushing them toward traditional banking methods or alternative financial solutions. As financial crimes become more sophisticated, banks must continuously enhance their cyber security frameworks, invest in advanced security technologies and implement robust risk management strategies to safeguard their operations and customer assets.

  Ultimately, mitigating cyber risks is essential to preserve the financial integrity of banks, ensuring seamless banking operations and maintaining public trust in the digital financial ecosystem.

- Interconnected effects across sectors: The consequences of cyber risks are rarely confined to a single domain. A cyber attack targeting a major financial institution can ripple through the economy, affecting businesses and bank's customers dependent on its services. Similarly, the erosion of trust in one sector can influence perceptions in others, creating a generalized fear of digital transactions or platforms. This interconnectedness underscores the importance of assessing and addressing the effects of cyber risks holistically.

By exploring these effects, this study seeks to underscore the critical importance of robust cyber security measures and their role in safeguarding financial system and individuals from the cascading impacts of cyber threats.

The Concept of 360-Degree Cyber Risk Management approach

In an era where technological advancements like cloud technologies, Internet of Things (IoT) devices and endpoint integration drive efficiency, convenience and productivity, cyber security risks grow proportionally. The paradox of technology and cyber security progressing inversely reveals a tradeoff that businesses must navigate carefully. While innovation fosters growth, it also introduces vulnerabilities that threaten asset security. Thus, organizations must adopt a proactive and comprehensive approach to cyber security, embracing the concept of 360-degree protection to safeguard their operations from ever-evolving cyber threats.

The 360-degree cyber risk management approach embodies a holistic methodology that addresses risks from every conceivable angle, ensuring both digital and physical assets are secure. This approach surpasses traditional data encryption and firewalls, emphasizing physical surveillance, employee training and proactive measures. By integrating this framework, businesses can mitigate vulnerabilities, detect threats and respond efficiently to incidents, fostering resilience against cyber attacks.

The Four Pillars of 360-Degree Cyber Risk Management approach

Prevention: As discussed, the cyber frauds and crimes have affected different industries, individuals and especially the banking sector. It has been witnessed different forms of cyber frauds like ATM frauds, Phishing, Denial of Service, Identity theft (Parthiban, L., & Manor, P. 2014). Prevention forms the cornerstone of 360-degree protection by actively monitoring systems and networks to detect and eliminates suspicious activities. Regular audits process, patch management and stringent access controls are essential to minimize vulnerabilities and pre-empt breaches.

Detection: Timely identification and detection of threats is critical. The conventional anomaly detection and rule-based techniques are two of the most popular utilized approaches for detecting cyber frauds, however, they are the time-consuming and resource-intensive approaches (Eyad Btoush et al. 2023). Identification of theft significantly impacts perceived security and trust in e-commerce business, leading to decreased consumer acceptance of new products and services provided by such businesses (K. I. 2013). Identifying the cyber fraud is an important aspect of fraud detection. Detecting fraud risks at an early stage can results investor protection, enhance investment returns, prevent costly legal battles and promote efficient operation (Menezes, A. 2024). Implementing robust backup solutions and data encryption helps ensure business continuity while safeguarding sensitive data. Early detection mechanisms enable swift responses, reducing the potential impact of cyber attacks.

Response: Organizations must develop and test incident response plans to react efficiently to security breaches. By coordinating efforts across teams and leveraging real-time intelligence, businesses can contain threats and minimize disruption.

Recovery: Recovery focuses on restoring operations post-incident. Regularly updating backups and streamlining recovery protocols ensure minimal downtime, enabling organizations to resume operations without compromising data integrity.

Benefits of a 360-Degree Cyber Risk Management approach

A 360-degree cyber risk management approach offers a comprehensive and proactive strategy for safeguarding bank's organizational assets from cyber threats. One of the important components of this approach is risk assessment, which involves conducting regular evaluations to identify vulnerabilities and assess the potential threats facing

an organization. This helps prioritize which risks need immediate attention and which can be managed over time, ensuring that resources are allocated efficiently to mitigate the most critical risks.

Network security is another crucial element of a robust cyber risk management strategy. This involves the proper implementation of various cyber security measures such as installation of firewalls, intrusion detection system and other tools to protect the network infrastructure from unauthorized access and malicious cyber attacks. By fortifying the network perimeter, organizations can reduce the likelihood of cyber intrusions that might compromise sensitive information.

The **Access control** procedure plays an important role in ensuring that only authorized personnel can access the systems and relevant data. This requires the enforcement of strict access policies, including multi-factor authentication system and role-based access control management, to eliminate the risk of unauthorized access or data breaches. Proper access management ensures that sensitive information remains protected and only permitted to the employees who needs it for their roles.

Maintaining **compliance** with cyber security regulations and standards is essential to reduce the legal and reputational risks. Organizations must adhere to industry-specific regulations such as General Data Protection Regulation (GDPR) or Health Insurance Portability and Accountability Act (HIPA) to ensure that they are meeting the necessary security standards and protecting their stakeholders interest. Non-compliance of such regulations can result in fines, legal consequences and damage to an organization's reputation. Therefore, the adherence to cyber security regulations are very crucial for risk management.

Vendor assessment is also an important aspect of cyber risk management process. As banks are increasingly relying on third-party vendors for various utilities services, it is essential to assess their security practices to ensure they meet the same cyber security standards as the bank itself maintain. Regular vendor security reviews help ensure that third-party relationships do not introduce additional vulnerabilities into the organization's security ecosystem.

Finally, a **communication plan** is necessary to foster cyber security awareness among employees and stakeholders. Educating staff about the organization's cyber security protocols and their individual roles in threat prevention is vital. Clear communication ensures that everyone is aware of potential risks and knows how to respond appropriately in the case of a cyber incident, thus, creating a more vigilant and informed workforce.

By implementing these measures, businesses can achieve robust security, ensuring operational continuity and safeguarding their reputation. The 360-degree approach to cyber risk management is an indispensable strategy for modern businesses. By addressing vulnerabilities at every level, fostering collaboration and prioritizing prevention and recovery, organizations can create a resilient cyber security framework. While eliminating cyber threats entirely may be impractical, mitigating risks and safeguarding assets comprehensively ensures continuity and trust in an increasingly digital world.

Proposing Preventive Measures leveraging a 360-degree approach for Enhanced Fraud Detection and Prevention

The increasing complexity and sophistication of cyber risks necessitate a proactive and comprehensive strategy to counteract them. This objective focuses on proposing preventive measures grounded in a 360-degree approach to enhance fraud detection and prevention across all levels in banking industry. A 360-degree approach emphasizes holistic coverage, integrating technological, organizational and individual-level measures to create a robust cyber security framework.

- **Building technological resilience:** Technology serves as the foundation of effective fraud detection and prevention systems. A comprehensive 360-degree approach encourages the use of various emerging tools such as Artificial Intelligence (AI) and Machine Learning (ML) algorithms to identify anomalies, detect suspicious patterns and predict potential fraud. Real-time monitoring of systems through platforms like 'Security Information and Event Management (SIEM)' ensures prompt detection and mitigation of threats.

  In addition to that, implementing efficient and high standard security measures such as multi-factor authentication, encryption protocols and regular updates to software and systems addresses vulnerabilities effectively. Integrating blockchain technology for secure transactions and immutable records further strengthens fraud prevention mechanisms, ensuring higher transparency and security in operations.

Practical steps for Implementation

Cyber security assessment: Conducting a thorough cyber security assessment is the first step towards building resilience. This step involves identifying potential threats and vulnerabilities, enabling organizations to develop targeted mitigation strategies. Regular assessments enhance the overall security posture and equip businesses to tackle emerging risks proactively.

Security Infrastructure: Adopting a borderless infrastructure model ensures seamless management of assets across diverse environment. Using advanced visibility and monitoring tools, organizations can identify and address even the most hidden vulnerabilities. A resilient infrastructure forms the core of effective fraud prevention.

Employee Training: An informed workforce acts as a critical line of defense against cyber threats. Regular training sessions should focus on educating employees about recognizing phishing scams, social engineering tactics and other fraudulent activities. Awareness and vigilance among employees significantly reduce the likelihood of successful attacks.

By integrating these technological and strategic measures, the banks can enhance their resilience against cyber frauds and threats while maintaining a secure operational environment.

- **Strengthening organizational practices:** For organizations, a 360-degree approach involves embedding cyber security into their culture and processes. This includes implementing strong governance frameworks, regular risk assessments and compliance with global cyber security standards such as ISO 27001. Establishing clear protocols for incident response, recovery and reporting ensures that cyber risks are managed effectively. Continuous employee training and awareness programs are crucial for minimizing human error and insider threats. Regular penetration testing and vulnerability assessments helps to identify and address potential weaknesses before they can be exploited.

- **Empowering individuals with awareness:** At the individual level, a 360-degree approach prioritizes education and awareness as key pillars of fraud prevention. This includes creating awareness among the users on safe digital practices, such as creating strong, unique passwords & credentials, recognizing phishing attempts and avoiding suspicious links. Educating banking customers and bank employees about cyber fraud risks, implementing multi-factor authentication system, utilizing encryption techniques and employing anomaly detection algorithms are some of the preventive measures (Natesan, G. 2024). Individuals must

be encouraged to use security tools like anti-virus software and personal firewalls. Public awareness campaigns and workshops can play a vital role in disseminating information about emerging threats and preventive measures, empowering individuals to protect themselves in the digital ecosystem.

- **Promoting collaboration and information sharing:** A comprehensive approach to fraud prevention also requires fostering collaboration between stakeholders, including Governments, financial institutions, corporates and cyber security firms. Sharing information about threats, vulnerabilities and attack methodologies through platforms such as industry consortiums and Government initiatives enhances collective preparedness. Public-private partnerships can facilitate the development of advanced cyber security technologies and policies, creating a unified front against cyber threats.
- **Continuous improvement through analytics and feedback:** A dynamic and adaptive approach is essential in the rapidly evolving cyber risk landscape. By implementing data analytics, the banking organizations can gain deeper insights into fraud detection trends and refine their preventive strategies. Feedback loops from past incidents and simulations can help in continuously updating and improving cyber security measures. This iterative process ensures that preventive frameworks remain effective against emerging threats.

By proposing preventive measures through a 360-degree approach, this study aims to establish a multi-layered defense mechanism that addresses the vulnerabilities of banks. Such a holistic framework not only enhances fraud detection and prevention but also builds resilience against the ever-evolving challenges of the cyber domain.

Regulatory Compliance and 360-degree Cyber Risk Management

Regulatory compliance is an important concern for banking organizations in India, whether they are private or public sector banks. Due to the rapid growth of the digital economy and increasing reliance on technology, India has witnessed a significant rise in cyber attacks and data breaches in recent years. Such incidents not only jeopardize the financial health of organizations but also tarnish their reputation in the highly competitive Indian market.

Indian organizations are also subject to strict legal frameworks such as the Information Technology (IT) Act, 2000, the Digital Personal Data Protection Act, 2023 (DPDP Act) and industry-specific regulations such as RBI guidelines. Non-compliance with these laws can result in heavy penalties, legal disputes and loss of trust among stakeholders.

Moreover, India's vibrant startup ecosystem and the growing number of Small and Medium Enterprises (SMEs) make it even more critical to prioritize data protection and cyber security measures. A robust 360-degree protection strategy ensures compliance with Indian regulations and safeguards sensitive data from unauthorized access, breaches and cyber threats.

Given the increasing adoption of digital payments, cloud computing and e-governance initiatives in India, implementing comprehensive cyber security measures is no longer a luxury but a necessity. Organizations must proactively adopt a holistic security approach to protect their operations, customers and stakeholders in the dynamic and challenging Indian business environment.

Challenges and Solutions in achieving 360-degree Cyber Risk Management approach

Many organizations perceive cyber security protection as an expensive endeavour. While there are low-

budget security solutions available, compromising on the quality of security for valuable company data is not advisable. Fortunately, achieving comprehensive 360-degree protection is both cost-effective and worth every investment.

Keeping pace with evolving cyber security trends poses a significant challenge for business leaders. Regularly monitoring industry updates and news is essential to maintain robust cyber security. However, many organizations mistakenly believe their current security measures are infallible. This false sense of security often arises in the absence of immediate threats. Unfortunately, cyber attacks can occur unexpectedly, making it crucial for businesses to continuously upgrade their security protocols. Implementing 360-degree protection is strongly recommended to address these challenges.

Organizational approach to 360-Degree Risk Management

The success of any cyber security program depends heavily on the collective efforts of the organization's team. While advanced digital systems play a pivotal role in threat detection and prevention, achieving comprehensive cyber security requires active participation from all team members.

For effective 360-degree cyber security, businesses must clearly define responsibilities, roles and communication channels within their teams to enforce necessary protocols. However, organizing these elements can be particularly challenging for large corporations with complex corporate structures and multiple branches. To address this, the formation of a robust cyber security framework is an essential first step.

By establishing a well-structured cyber security strategy and fostering collaboration across teams, organizations can create a resilient defense system capable of mitigating risks and ensuring regulatory compliance.

Conclusion

In an era of digital transformation, cyber threats demand a proactive and multi-faceted response. This study emphasizes the necessity of a 360-degree cyber risk management approach for robust fraud detection and prevention, particularly, in the banking sector. By integrating technological innovations like machine learning, encryption and real-time monitoring with organizational and individual preparedness, this strategy ensures a holistic defense against cyber risks. Regular risk assessments, compliance with regulatory frameworks and collaboration across stakeholders are vital in addressing vulnerabilities. Furthermore, continuous workforce education and vendor evaluations strengthen systemic resilience.

The suggestions from this article include prioritizing investments in adaptive technologies and fostering public-private partnerships to enhance information sharing and collective preparedness. Promoting digital literacy among customers and emphasizing cyber security at organizational and policy levels can mitigate risks more effectively. Embracing this comprehensive approach enables organizations to stay ahead of evolving threats, ensuring operational continuity, safeguarding reputations and fostering trust among stakeholders in a dynamic digital ecosystem.

References

Roy, N., and P., S. (2024). Proactive cyber fraud response: a comprehensive framework from detection to mitigation in banks. Digital Policy, Regulation and Governance. https://doi.org/10.1108/dprg-02-2024-0029.

Roy, N., and Prabhakaran, S. (2022). Internal-led cyber frauds in Indian banks: an effective machine learning-based defense system to fraud detection, prioritization and prevention. Aslib Journal of Information Management, 75, 246-296. https://doi.org/10.1108/ajim-11-2021-0339.

Natesan, G. (2024). Prevention of Cyber Frauds in the Banking Sector. International Scientific Journal of Engineering and Management. https://doi.org/10.55041/isjem01341.

Eyad Btoush et al. (2023). A systematic review of literature on credit card cyber fraud detection using machine and deep learning. PeerJ-Computer Science, 9. https://doi.org/10.7717/peerj-cs.1278.

Emad Tariq et al. (2024). How cybersecurity influences fraud prevention: An empirical study on Jordanian commercial banks. International Journal of Data and Network Science. https://doi.org/10.5267/j.ijdns.2023.10.016.

Shewangu Dzomira et al. (2017). Cyber-banking fraud risk mitigation conceptual model. Banks and Bank Systems, 10.

L. Parthiban et al. (2014). The effect of cybercrime on a Bank's finances.

Tan, H. (2002). E-Fraud: Current Trends and International Developments. Journal of Financial Crime, 9, 347-354. https://doi.org/10.1108/EB026034.

K. I (2013). The Impact of Identity Theft on Perceived Security and Trusting E-Commerce.

Menezes, A. (2024). A Postmortem of Financial Frauds: The 5S Approach. Economic Affairs. https://doi.org/10.46852/0424-2513.3.2024.29.

https://www.thehindu.com/data/cyber-fraud-in-banking-transactions-surges-in-fy24-data/article68813626.ece

BANK QUEST THEMES

The themes for "Bank Quest" are identified as:

1. **April - June, 2025: Net Zero Banking**

   Sub-themes: Responsible Banking, Green Finance, Green Bonds, Transition to Green Financing

2. **July - September, 2025: Strategic HRM Initiatives for Banks**

   Sub-themes: Talent Management, Succession Planning, Employee Engagement Strategy, Diversity and Inclusion Management, HR Audit

3. **October - December, 2025: Emerging Technologies in Banking**

   Sub-themes: Applications of Generative Artificial Intelligence (AI), Ethical AI, Fraud Detection and Creating Early Warning Signals, Technologies for Project Appraisal and Credit Appraisal

4. **January - March, 2026: New Avenues of Payments Systems**

   Sub-themes: UPI, ULI, CBDC- Challenges, Opportunities and Prospects, Cyber Security

5. **April - June, 2026: Financial Inclusion – The Next Phase**

बचत और निवेश: बढ़ती संभावनाएं

✍ संजय मधुकर नाफड़े*

बचत और निवेश दो भिन्न विचार हैं, लेकिन व्यवहार में दोनों विचार एक दूसरे के पूरक भी हैं। सामान्यत: हम निवेश करने से पहले बचत करते हैं, जिसका अर्थ है बाद में उपयोग के लिए धन अलग रखना। जबकि निवेश, इस उम्मीद के साथ किया जाता है कि इससे आय में वृद्धि होगी या निवेश के मूल्य में वृद्धि होगी। बचत हमारे जीवन में कई प्रकार से महत्वपूर्ण हो सकती है, जैसे आपातकालीन स्थितियों, अल्पकालिक और दीर्घकालिक लक्ष्यों के लिए पैसे बचाना। भविष्य के उपयोग के लिए पैसे अलग रखना हमें जीवन के लक्ष्यों को पूरा करने में मदद कर सकता है। वित्तीय लक्ष्य प्रत्येक व्यक्ति के लिए अलग-अलग महत्व रखते हैं, यह विवाह के लिए पर्याप्त बचत करना या कर्ज कम करने या सिर्फ सेवानिवृति पश्चात् जीवन के लिए बचत करना हो सकता है। वित्तीय लक्ष्य निर्धारित करने का उद्देश्य बचत को सार्थक बनाना और बचत को अपने वित्तीय लक्ष्यों तक पहुँचने की दिशा में लगाना है। यह इस बात का अनुमान लगाने में मदद करता है कि आप अपनी बचत से क्या करना चाहते हैं, जो तभी प्रभावी हो सकता है जब यदि हमारे पास स्पष्ट रूप से परिभाषित लक्ष्य हो।

नियमित रूप से बचत करना और समय के साथ अनुशासित तरीके से इस राशि का निवेश करना अपने लक्ष्य तक पहुँचने में मदद कर सकता है। सही अर्थों में बचत, वित्तीय सुरक्षा प्राप्त करने की दिशा में एक महत्वपूर्ण कदम है। अपने वित्त पर नियंत्रण रखने के लिए, अपने वर्तमान और भविष्य के वित्तीय जीवन को सुरक्षित करने के लिए एक सुव्यवस्थित बचत आदत विकसित करना आवश्यक है। बचत प्रत्येक के लिए उपयोगी है, क्योंकि इससे आप निवेश के सही मिश्रण तक पहुँचते हैं जो किसी को भी समय पर अपने सभी वित्तीय लक्ष्यों को प्राप्त करने में मदद कर सकता है। कभी-कभी, यह कल्पना करना कठिन होता है कि आप बचत के लिए पैसे कहाँ से ला सकते हैं। लेकिन, अपने खर्च और बचत योजना पर नज़र डालकर शुरुआत कर सकते है। आप अपने लक्ष्यों के आधार पर अपने खर्च को अलग तरह से प्राथमिकता देने, मौजूदा खर्चों में कटौती करने, अतिरिक्त आय का रास्ता खोजने, उपहार के पैसे, बोनस जैसे उपायों से बचत का फैसला कर सकते हैं।

बचत और निवेश दोनों ही एक स्वस्थ वित्तीय योजना के महत्वपूर्ण घटक हैं। बचत एक सुरक्षा जाल और अल्पकालिक लक्ष्यों को प्राप्त करने का एक तरीका प्रदान करती है, जबकि निवेश में उच्च दीर्घकालिक रिटर्न की क्षमता होती है और यह दीर्घकालिक वित्तीय लक्ष्यों को प्राप्त करने में मदद कर सकता है। हालाँकि, निवेश करने से पैसे खोने का जोखिम भी होता है। प्रत्येक दृष्टिकोण के अपने फायदे और नुकसान हैं और यह सही संतुलन खोजना महत्वपूर्ण है जो हमारी वित्तीय स्थिति और लक्ष्यों के लिए काम करता है। अंतत: एक अच्छी तरह से विकसित दृष्टिकोण जिसमें बचत और निवेश दोनों शामिल हो, धन में वृद्धि करने, वित्तीय संकटों से बचाने और अधिक सुरक्षित वित्तीय भविष्य के लिए एक ठोस आधार प्रदान करने में मदद कर सकता है। यह एक मिथक है कि बचत अर्थात् खर्च के बाद अपनी आय से बचा हुआ धन, लेकिन बदलते आर्थिक परिदृश्य तथा बेहतर बचत व निवेश के उपकरणों ने इस अवधारणा

*सेवानिवृत्त मुख्य प्रबंधक, स्टेट बैंक ऑफ इंडिया।

को बदल दिया है। अब दूरदर्शी बचतकर्ता पहले अपनी आय का एक बड़ा हिस्सा बचाते हैं, फिर बचे हुए पैसे को खर्च में इस्तेमाल करते हैं। इस सरल बदलाव के साथ, व्यक्ति अब नियमित रूप से बचत करने और अधिक बचत करने में सक्षम हैं। लेकिन, मात्र बचत करना अब लाभप्रद नहीं रह गया है, खासकर तब जब मुद्रास्फीति इस पर गहरा प्रभाव डालती है। ऐसे समय में जब बचत बैंक खाते और सावधि जमा से निश्चित रिटर्न लगातार कम हो रहा है, आपकी बचत को भविष्य के मूल्य को बनाए रखने के लिए मुद्रास्फीति मिलान लाभ अर्जित करने की आवश्यकता है। हालाँकि, आपके पास भविष्य के वित्तीय लक्ष्य भी हैं, जिसके लिए आपको अपनी ज़रूरत के मूल्य तक पहुँचने के लिए मूल्य में वृद्धि की आवश्यकता होती है।

बचत बनाम निवेश

वित्तीय सुरक्षा और उज्ज्वल भविष्य सुनिश्चित करने के लिए बचत और निवेश के बीच अंतर को समझना आवश्यक है। हालाँकि सामान्य बातचीत में बचत और निवेश को कभी-कभी एक-दूसरे के लिए उपयोग किया जाता है, लेकिन यह ध्यान रखना महत्वपूर्ण है कि यह दोनों बहुत अलग हैं। बचत और निवेश दोनों ही व्यक्तिगत वित्त के महत्वपूर्ण तत्व हैं, और इसे जल्दी प्रारम्भ करना दीर्घकालिक वित्तीय स्थिरता के लिए खुद को तैयार करने का एक बेहतर तरीका है। बचत और निवेश दोनों ही किसी व्यक्ति के व्यक्तिगत वित्त-योजना के लिए महत्वपूर्ण हैं।

- बचत करने का अर्थ है उसे सुरक्षित तरीके से संग्रहीत करना ताकि जब हमें इसकी आवश्यकता हो तो यह उपलब्ध हो तथा इसका मूल्य कम होने का जोखिम भी कम हो।
- निवेश में जोखिम तो है, लेकिन उच्च रिटर्न की संभावना भी है।
- निवेश आमतौर पर लंबी अवधि के लिए किया जाता है, जैसे कि बच्चों की उच्च शिक्षा, परिसंपत्ति खरीदने या किसी की सेवानिवृत्ति के बाद के लिए।

बचत क्या है?

यह देखा गया है कि महंगी वस्तुओं की खरीददारी और आपातकालीन स्थिति दोनों के लिए बचत की जाती हैं। बचत व्यक्तिगत वित्त का एक अनिवार्य हिस्सा है जिसमें भविष्य के उपयोग के लिए पैसे अलग रखना शामिल है। दशकों पहले यद्यपि बचत कम ही थी परन्तु प्राय: घर में ही रखी जाती थी, अभी बचत खाते या जमा प्रमाणपत्र का उपयोग किया जा सकता हैं जो समय के साथ ब्याज अर्जित करता है। बचत अल्पकालिक वित्तीय लक्ष्यों को पूरा करने जैसे कि कोई नया गैजेट खरीदना, भ्रमण पर जाना या अप्रत्याशित खर्चो के लिए आपातकालीन निधि रखने के लिए की जाती है। नियमित रूप से पैसे अलग रखकर, आप एक ऐसा कुशन बना सकते हैं जो आपको कठिन समय से निपटने में मदद कर सकता है। बचत आमतौर पर कम जोखिम रखती है, जिसका अर्थ है कि आपका पैसा सुरक्षित है, लेकिन प्राप्त ब्याज दरें भी कम हैं। आमतौर पर बचत को लगभग एक वर्ष या उससे कम की अवधि माना जाता है। कम अवधि के लिए रखते समय भी यह ध्यान में रखा जाना चाहिए कि कब धन की आवश्यकता होगी, धन के लिए योजना क्या है और लक्ष्य से जुड़ी सुरक्षा/जोखिम क्या है।

बचत के पक्ष और विपक्ष

बचत के कई लाभ हैं जैसे कि अप्रत्याशित घटनाओं के लिए वित्तीय सुरक्षा जाल प्रदान करना, खरीदारी और अन्य अल्पकालिक लक्ष्यों के लिए तरलता प्रदान करना और नुकसान से सुरक्षित रहना। इससे आपातकालीन निधि का निर्माण किया जा सकता है। इसमें नुकसान का न्यूनतम जोखिम होता है क्योंकि बैंकों में रखी गई बचत पाँच लाख रुपये तक बीमा गारंटी द्वारा संरक्षित है। हालाँकि, विचार करने पर बचत में कुछ कमियाँ भी हैं, जैसे कि जोखिम भरे निवेशों से संभावित उच्च रिटर्न से चूक जाना। लम्बी अवधि में बढ़ती मुद्रास्फीति के कारण बचत भी क्रय शक्ति खो सकती है। हालांकि बचत किसी भी वित्तीय योजना का एक महत्वपूर्ण हिस्सा है, लेकिन वित्तीय नियोजन के लिए एक

संतुलित दृष्टिकोण प्राप्त करने के लिए इसे निवेश के अन्य रूपों, जैसे सेवानिवृत्ति खातों या शेयर बाजार में निवेश के साथ जोड़ना आवश्यक है। यह जोखिमपूर्ण तो है लेकिन उच्च लाभ देने वाली परिसंपत्तियों में निवेश न करने पर अवसर लागत की हानि संभव है।

बचत के अवसर

एक तरफ, सही जगह पर पैसा निवेश करना धन निर्माण की प्रक्रिया में आपकी सहायता कर सकता है। दूसरी ओर, नए निवेशकों को यह सलाह दी जाती हैं कि वे केवल उस हिस्से का निवेश करें जो उनके पास अपने आपातकालीन धन को अलग करने के बाद बच जाता है। (बचत और निवेश बहुत अलग हैं और इसको उस दृष्टि से देखा जाना तथा समझना आवश्यक है। इसका परिणाम यह हो सकता है कि आप निवेशक के रूप में अधिक सफलता प्राप्त करें। अनिवार्य रूप से, बचत और निवेश दोनों मौद्रिक मूल्य रखते हैं जो वित्तीय साधनों के रूप में प्रकट होता है।) नकद, जमा प्रमाण पत्र, आवर्ती जमा तथा अल्पावधि सावधि जमा आदि कुछ सामान्य उपकरण हैं जिनका उपयोग बचत के उद्देश्य के लिए किया जाता है।

बचत खाता

बचत खाता सबसे पसंदीदा वित्तीय साधनों में से एक है जो देश में प्रत्येक बैंक द्वारा सामान्य जनता के लिए उपलब्ध किया जाता है। खाता धारक पैसे जमा कर सकते हैं और जमा किए गए धन से ब्याज कमा सकते हैं। विश्वसनीयता, उच्च तरलता दर, आसान पहुंच और जमा और निकासी पर कोई सीमा नहीं होने के कारण यह सबसे पसंदीदा जमा विकल्पों में से एक है। भारतीय बैंकों द्वारा कई प्रकार के बैंक खाते उपलब्ध कराए जाते हैं, जिनमें से बचत खाता सबसे ज़रूरी बैंक खातों में से एक है, जहाँ व्यक्ति पैसे जमा कर सकते हैं और अच्छा ब्याज कमा सकते हैं। ये खाते आपके पैसे जमा करने के लिए एक सुरक्षित जगह प्रदान करते हैं।

बचत खाते पर सामान्य ग्राहकों को दी जाने वाली ब्याज दर 2.00% से 7.00% के बीच है, लेकिन वरिष्ठ नागरिक ग्राहकों को नियमित दरों से 0.50% अधिक अतिरिक्त ब्याज दर प्रदान की जाती है। 5 लाख रुपये तक की बैंक जमा राशि डिपॉजिट इंश्योरेंस एंड क्रेडिट गारंटी कॉरपोरेशन द्वारा बीमाकृत है, अत: यह अधिक सुरक्षित है। इसमें यह सुविधा है कि खाता धारक जितनी बार चाहे उतनी बार धन हस्तांतरित करने या निकालने के लिए उच्च तरलता सुनिश्चित करता है, साथ ही खाता धारक को उसी बैंक में बचत खाते को सावधि जमा के साथ जोड़ने की सुविधा भी है। बचत खाता धारकों को ऑनलाइन भुगतान या नकद निकासी के लिए एटीएम या डेबिट कार्ड प्रदान किए जाते हैं, साथ ही यह उपयोगकर्ताओं को यूपीआई, एनईएफटी (राष्ट्रीय इलेक्ट्रॉनिक निधि अंतरण), आरटीजीएस (वास्तविक समय सकल निपटान), आईएमपीएस (तत्काल भुगतान सेवा), नेट बैंकिंग, मोबाइल बैंकिंग या शाखा में जाकर निधि अंतरण करने की सुविधा भी देता है।

यह उपयोगकर्ताओं को नेट बैंकिंग, मोबाइल बैंकिंग, एसएमएस बैंकिंग आदि के माध्यम से अपने बचत खाते को संचालित करने में सक्षम बनाता है। जमा की जाने वाली राशि पर कोई सीमा नहीं लगाई जाती, लेकिन खाता धारकों को मासिक औसत शेष आवश्यकताओं का पालन करना होता है। बचत खाता जमा और उससे जुड़े डेबिट कार्ड पर विभिन्न छूट और सुविधाएं प्रदान करता है। इस खाते में खाता धारक द्वारा ब्याज भुगतान विकल्प चुना जा सकता है - मासिक, त्रैमासिक, अर्ध-वार्षिक और वार्षिक। बचत खाते कई प्रकार के हो सकते है, विभिन्न बैंकों ने उनको अलग नाम भी दिए है साथ ही भिन्न प्रकार की सुविधाएं भी प्रदान की है, जैसे नियमित बचत खाता, जीरो बैलेंस या बेसिक सेविंग्स बैंक डिपॉजिट अकाउंट, वरिष्ठ नागरिक बचत खाता, महिला बचत खाता,बच्चों का बचत खाता, डिजिटल बचत खाता, वेतन खाता, पारिवारिक बचत खाता।

आवर्ती जमा (आरडी)

यह सबसे अधिक प्रचलित अल्पावधि निवेश विकल्प है और

यह सभी बैंकों में उपलब्ध है, इसलिए कई लोग अल्पावधि प्रयोजनों के लिए इसका उपयोग करते हैं। यह योजना कम राशि से भी बचत करने को प्रोत्साहित करती है यह आपको अपने निवेश पर परिपक्व होने तक एक निश्चित दर से ब्याज कमाने देता है। इसमें निवेश पर प्रतिफल 4% से 6% प्रति वर्ष तक प्राप्त हो सकता है, इसकी समय सीमा प्राय: 6 महीने से 10 वर्ष तक हो सकती है। वर्तमान में पारस्परिक फंड्स की बढ़ती लोकप्रियता के कारण आवर्ती जमा को एसआईपी के माध्यम से अधिक चुनौती मिल रही है।

निश्चित आय खाते (सावधि जमा)

सावधि जमा (एफडी) बैंकों के लिए अल्पकालिक निवेश के लिए धन जुटाने की एक अन्य सामान्य तकनीक है, यह धनराशि एक निश्चित अवधि के लिए, आमतौर पर 1 से 10 वर्ष के लिए, पूर्व निर्धारित रिटर्न दर पर निवेश की जाती है, जिसके बाद यह परिपक्व हो जाती है और इसे निकाला जा सकता है। बचत के लिए एक वर्ष की सावधि जमा पर्याप्त कही जा सकती है। यद्यपि बचत खातों और आवर्ती जमा की तुलना में ब्याज दरें अधिक होती हैं, लेकिन समय से पहले निकासी संभव नहीं है या पेनाल्टी देकर भुगतान लिया जा सकता है। इसमें वार्षिक रिटर्न दर: 2.5% से 7.5% तक हो सकती है। यह बचत का सबसे पसंदीदा उपकरण है, इस समय भारतीय बैंकों की कुल सावधि जमाओ में एक बड़ी हिस्सेदारी वरिष्ठ नागरिकों की है, जिसे वे अधिक सुरक्षित मानते है। एक वर्ष से अधिक अवधि की सावधि जमाएं भी बैंकों में उपलब्ध है लेकिन वह फिर दीर्घावधिक निवेश माना जाता है।

निगमों द्वारा की गई जमा राशि (सीडी)

कॉर्पोरेट सावधि जमाएं बैंक सावधि जमाओ के समान ही होती हैं, अंतर यह है कि इन्हें निगमों द्वारा विस्तार और परिचालन के लिए एकत्र किया जाता है। चूंकि इसमें चूक का खतरा अधिक होता है, इसलिए ब्याज दरें बैंक एफडी की तुलना में थोड़ी अधिक होती हैं। जो लोग अधिक जोखिम सहन कर सकते हैं, वे कॉर्पोरेट एफडी में निवेश कर सकते

निवेश क्या है?

निवेश में बचत खातों की तुलना में अधिक रिटर्न की संभावना होती है, चक्रवृद्धि ब्याज और पुनर्निवेश के माध्यम से समय के साथ आपकी संपत्ति में वृद्धि करने की क्षमता होती है तथा यह आपको सेवानिवृत्ति के लिए बचत करने या घर खरीदने जैसे दीर्घकालिक वित्तीय लक्ष्यों को प्राप्त करने में मदद करने का अवसर प्रदान करता है। निवेश में हमेशा कुछ हद तक जोखिम शामिल होता है और इस बात की कोई गारंटी नहीं है कि आपको लाभ ही मिलेगा या आपने जो निवेश किया है, वह पूर्ण वापस मिलेगा। इसके लिए कई स्वामित्व में विविधता लाने से जोखिम कम करने में मदद मिल सकती है। इस पर शोध करना और विभिन्न प्रकार के निवेशों से जुड़े संभावित जोखिमों को समझना महत्वपूर्ण है। निवेश के लिए अनुशासन और दीर्घकालिक दृष्टिकोण की आवश्यकता होती है, इस कारण कुछ लोगों के लिए बाजार की अस्थिरता या जल्दी लाभ कमाने के प्रयास में भीड़ का अनुसरण करने के प्रलोभन के सामने बनाए रखना मुश्किल हो सकता है। इससे पहले कि आप कोई भी पैसा निवेश में लगाएं, सुनिश्चित करें कि आपके पास आपातकालीन निधि में कई महीनों के खर्चों को पूरा करने के लिए पर्याप्त बचत हो तथा आपके बचत खाते में बिल, किराया और किराने का सामान जैसी आपकी सभी अल्पकालिक आवश्यकताओं को पूरा करने के लिए पर्याप्त धन हो।

निवेश के अवसर

निवेश में बचत की तुलना में अधिक रिटर्न की संभावना होती है, साथ ही इससे दीर्घकालिक वित्तीय लक्ष्य प्राप्त करने में मदद मिल सकती है। अपने पोर्टफोलियो के विविधीकरण से जोखिम कम हो सकता है। निवेश के लिए बाजार में स्टॉक्स, बॉन्ड, इक्विटी, यूलिप और म्यूचुअल फंड जैसे विभिन्न निवेश साधन उपलब्ध हैं। निवेश जोखिमों से मुक्त नहीं है, यदि उचित योजनाओं, स्टॉक्स और निधियों में निवेश नहीं किया तो हानि का जोखिम हो सकता है, अल्पावधि ही नहीं बल्कि दीर्घ अवधि का निवेश भी जोखिम युक्त हो

सकता है, निवेश में लम्बे समय और धैर्य की आवश्यकता होती है। बचत में बहुत कम जोखिम होता है। दूसरी और, निवेश में पैसा खोने का जोखिम होता है। इसलिए, सामान्य तौर पर निवेश करना, बचत से ज़्यादा जोखिम भरा होता है। यह जोखिम अपने पोर्टफोलियो के विविधीकरण से कुछ हद तक कम किया जा सकता है।

डेट म्यूचुअल फंड

डेट म्यूचुअल फंड अल्पावधि के लिए मुख्य रूप से ऋण साधनों जैसे सरकारी बांड, वाणिज्यिक पत्र, ट्रेजरी बिल, कॉर्पोरेट बांड और अन्य मुद्रा बाजार साधनों में निवेश करते हैं। उच्च अल्पावधि म्यूचुअल फंड की तलाश करने वाले जोखिम से बचने वाले निवेशकों के लिए, यह सबसे बड़ी अल्पावधि निवेश संभावनाओं में से एक है। इसमें निवेश पर प्रतिफल 8% से 11% प्रति वर्ष प्राप्त हो सकता है लेकिन इसके लिए 6 महीने से 3 वर्ष तक इंतज़ार भी करना पड़ सकता है। यदि आप तीन वर्षों के भीतर यूनिट्स को भुनाते हैं तो अल्पकालिक म्यूचुअल फंड पर कर लगाया जाता है, लेकिन यदि आप यूनिट्स को तीन वर्षों से अधिक समय तक रखते हैं तो दीर्घकालिक पूंजीगत लाभ पर कर लगाया जाता है।

इक्विटी म्यूचुअल फंड में व्यवस्थित निवेश

आप अपनी जोखिम क्षमता और निवेश समय सीमा को पूरा करने के लिए विभिन्न परिसंपत्ति वर्गों में व्यापक निवेश विकल्प के लिए म्यूचुअल फंड में निवेश कर सकते हैं। ऐसे फंड उपलब्ध हैं जो अल्पकालिक, मध्यम और दीर्घकालिक वित्तीय लक्ष्यों और अलग-अलग जोखिम ग्रेड के लिए उपयुक्त हैं। इसके अलावा, आप म्यूचुअल फंड में निवेश करने के लिए इसकी सुविधा और संरचना के लिए एक व्यवस्थित निवेश योजना या एसआईपी का उपयोग कर सकते हैं। चूंकि अधिकांश लोगों को मासिक आय प्राप्त होती है, इसलिए वे म्यूचुअल फंड में निवेश करने के लिए एसआईपी मार्ग चुनकर अपने वित्तीय लक्ष्यों की ओर मासिक निवेश चक्र का उपयोग कर सकते हैं। यह आपके बचत अनुशासन को एक पायदान ऊपर ले जाता है - आप न केवल नियमित रूप से बचत करते हैं, बल्कि नियमित रूप से निवेश भी करते हैं। व्यवस्थित निवेश योजनाएं (एसआईपी) लंबी अवधि के लिए सर्वोत्तम हैं, हालांकि अच्छे रिटर्न पाने के लिए इनका प्रयोग छोटी अवधि के लिए भी किया जा सकता है। यदि आपके पास एक वर्ष का निवेश क्षितिज है और आप एक अच्छा अल्पावधि निवेश चाहते हैं, तो लार्ज-कैप म्यूचुअल फंड में एसआईपी की सिफारिश की जाती है क्योंकि वे बड़ी कंपनियों में निवेश करते हैं जो बाजार में तेजी से बढ़ सकते हैं। निवेश पर प्रतिफल 8% से 15% प्रति वर्ष प्राप्त हो सकता है, उच्च प्रतिफल के लिए 6 महीने से 5 वर्ष का समय देना होगा। डेट म्यूचुअल फंड की तरह, इक्विटी म्यूचुअल फंड के रिटर्न की गणना अल्पकालिक और दीर्घकालिक पूंजीगत लाभ का उपयोग करके की जाती है।

पारस्परिक निधियां भारतीयों के लिए निवेश करने और उनके संपत्ति को बढ़ाने का एक अधिक लोकप्रिय तरीका बन गई हैं। ये निवेश वाहन एक पोर्टफोलियो बनाने के लिए एक सुविधाजनक और विविध दृष्टिकोण प्रदान करते हैं। भारतीय म्यूचुअल फंड उद्योग की एयूएम मई 2024 में, ₹58.60 ट्रिलियन तक पहुंच चुकी है। यह आंकड़ा देश की अपार वृद्धि और म्यूचुअल फंड की लोकप्रियता को दर्शाता है। मई 2024 तक, इंडियन म्यूचुअल फंड उद्योग की एसेट अंडर मैनेजमेंट (एयूएम) की राशि ₹58,91,160 करोड़ की स्थिति में थी। पिछले दशक में, उद्योग के एयूएम में एक उल्लेखनीय वृद्धि हुई है, जो मई 2014, को ₹10.11 ट्रिलियन से लगभग छह गुना बढ़कर मई, 2024 को ₹58.91 ट्रिलियन हो गई है। पिछले पांच वर्षों में विकास विशेष रूप से महत्वपूर्ण रहा है। मई 2019 से मई 2024 तक, उद्योग का एयूएम दोगुने से अधिक, ₹25.94 ट्रिलियन से बढ़कर ₹58.91 ट्रिलियन हो जाता है। यह तेज़ विस्तार म्यूचुअल फंड में भारतीय निवेशकों द्वारा किए गए स्वीकृति और विश्वास को दर्शाता है। आंकड़ों के अनुसार उद्योग की कुल एयूएम में एसआईपी की हिस्सेदारी लगभग बीस

प्रतिशत हो गयी है, इसके खातों की संख्या भी 9.34 करोड़ हो चुकी है और निवेशित धन राशि भी ₹23,300 करोड़ हो चुकी है।

पारस्परिक निधि उद्योग ने कई महत्वपूर्ण पड़ाव हासिल किए है। मई 2014 में, उद्योग का एयूएम पहली बार ₹10 लाख करोड़ से बढ़ गया और लगभग तीन वर्षों के भीतर, इसने अगस्त 2017 में ₹20 लाख करोड़ का आंकड़ा पार कर दिया। यह गति आगे भी जारी रही और नवंबर 2020 तक, एयूएम ₹30 लाख करोड़ से अधिक का हो गया था। 31 मई, 2024 तक, म्यूचुअल फंड उद्योग का एयूएम प्रभावशाली ₹58.91 लाख करोड़ पर खड़ा था। म्यूचुअल फंड उद्योग ने मई 2021 में 10 करोड़ फोलियो तक पहुंचकर एक महत्वपूर्ण उपलब्धि भी चिह्नित की, जो व्यक्तिगत निवेशकों की बढ़ती भागीदारी को दर्शाता है। मई 31, 2024 तक, कुल खातों की संख्या 18.60 करोड़ (186 मिलियन) तक पहुंच गई है। विशेष रूप से, इक्विटी, हाइब्रिड और सॉल्यूशन ओरिएंटेड स्कीम के तहत खातों की संख्या, जो मुख्य रूप से खुदरा निवेशकों द्वारा चलाई जाती हैं, लगभग 14.90 करोड़ (149 मिलियन) थी। यह मजबूत खुदरा निवेशकों की उपस्थिति म्यूचुअल फंड के प्रति बढ़ती जागरूकता और उसको एक व्यवहार्य निवेश विकल्प के रूप में प्रतिपादित करती है (एम्फी के अनुसार)।

स्टॉक एक्सचेंज

शेयर बाजार उच्च जोखिम लेने वालों के लिए आदर्श अल्पकालिक निवेश है जो अपनी कमाई को अधिकतम करना चाहते हैं। यदि आप सही स्टॉक पहचान सकें तो आप उनमें कुछ महीनों के लिए निवेश करके अपना पैसा दोगुना कर सकते हैं। यदि आप गलत स्टॉक पर दांव लगाते हैं, तो आपको अपना पूरा निवेश खोने का खतरा रहता है। यह जानने के लिए कि भारत में अल्पावधि में खरीदने के लिए सबसे अच्छे स्टॉक कौन से हैं, आपको इस बाजार पर तीक्ष्ण दृष्टि और शोध की आवश्यकता होती है इस बाजार में लाभ की कोई सीमा नहीं है, सब कुछ आपके चुनाव तथा जोखिम लेने की क्षमता पर निर्भर करता है। उदाहरण के लिए, मान लीजिए कि आप किसी बड़ी कंपनी में निवेश करना चाहते हैं। इसके शेयर खरीदकर, आप कंपनी के एक छोटे से हिस्से के मालिक बन सकते हैं और इसके विकास और मुनाफे से लाभ उठा सकते हैं। अगर वह कंपनी अच्छा प्रदर्शन करती है, तो समय के साथ इसके शेयर का मूल्य बढ़ सकता है, जिससे आप इसे लाभ के लिए बेच सकते हैं। याद रखने वाली एक महत्वपूर्ण बात यह है कि निवेश करने से कोई गारंटी नहीं मिलती है और हमेशा पैसे खोने का जोखिम रहता है। उदाहरण के लिए, अगर वह कंपनी दिवालिया हो जाए, तो आपका निवेश लगभग बेकार हो सकता है। इसलिए अपने जोखिम को कम करने के लिए अलग-अलग कंपनियों और उद्योगों में निवेश करके अपने पोर्टफोलियो में विविधता लाना ज़रूरी है।

शेयर बाजार की समीक्षा

30 शेयरों वाला बीएसई सेंसेक्स वित्त वर्ष 2024 के आखिरी दिन (गुरुवार, 28 मार्च) को करीब 655.04 अंक यानी 1% की बढ़त के साथ 73,651.35 के स्तर पर बंद हुआ। वित्त वर्ष 2024 के दौरान, एसएंडपी बीएसई सेंसेक्स इंडेक्स ने कई रिकॉर्ड ऊंचाई को छूआ है और बीएसई-सूचीबद्ध कंपनियों का बाजार पूंजीकरण नवंबर 2023 में पहली बार ₹333 लाख करोड़ यानी 4 ट्रिलियन डॉलर को पार कर गया है। वित्त वर्ष 2024 में पांच साल की अवधि के दौरान बीएसई सेंसेक्स में 24.85% की दूसरी सबसे बड़ी वृद्धि हुई है; वित्त वर्ष 2021 में 68.01% की सबसे बड़ी वृद्धि दर्ज की गई थी। वित्त वर्ष 2023 में एसएंडपी बीएसई सेंसेक्स में मात्र 0.72% की वृद्धि देखी गई।

बाजार विशेषज्ञों का मानना है कि वित्त वर्ष 24 भारतीय शेयर बाजारों के लिए एक उत्कृष्ट वर्ष रहा, जिसमें बीएसई सेंसेक्स में लगभग 24% की अविश्वसनीय वृद्धि देखी गई, जो पिछले वर्षों के प्रदर्शन से बेहतर रहा और निवेशकों को पर्याप्त धन अर्जित हुआ। यह वृद्धि कई वैश्विक समकक्ष की तुलना में अधिक है, जो बाजार के लचीलेपन और ताकत

को दर्शाता है। बाजार विशेषज्ञों का मानना है कि मजबूत आर्थिक वृद्धि और ठोस कॉर्पोरेट नतीजों सहित कई संभावित उद्येलकों ने तेजी के रुझान में महत्वपूर्ण योगदान दिया और निवेशकों का उत्साह बढ़ाया है। इसके अलावा, घरेलू और विदेशी संस्थागत निवेशकों दोनों की ओर से मजबूत निवेश ने पूरे साल बाजार की धारणा को और मजबूत किया। एक अन्य कारक, जिसने इसमें योगदान दिया वह था आईपीओ बाजार, जो वित्त वर्ष 24 के दौरान फला-फूला, जिसमें लगभग 75 नए इश्यू लॉन्च होने के साथ गतिविधि में उछाल देखा गया। भारतीय अक्षय ऊर्जा विकास एजेंसी, नेटवेब और सिग्नेचर ग्लोबल जैसी कंपनियों ने लिस्टिंग के बाद 150% से अधिक का रिटर्न दिया, जिससे बाजार में तेजी का माहौल बना। औसत लिस्टिंग लाभ में 29% की उल्लेखनीय वृद्धि देखी गई, जो इन नई पेशकशों के लिए निवेशकों के उत्साह को रेखांकित करता है।

वित्त वर्ष 2024 में सेंसेक्स शेयरों का प्रदर्शन

उपलब्ध आंकड़ों के अनुसार, 30 शेयरों में से 28, वित्तीय वर्ष 2024 के अंतिम दिन लाभ के साथ बंद हुए। टाटा मोटर्स लिमिटेड ने 30-शेयर बीएसई सेंसेक्स पैक का नेतृत्व किया, जो वित्त वर्ष 24 में 147.2% के लाभ के साथ एक मल्टीबैगर स्टॉक में बदल गया। लाभ पाने वालों की सूची में शामिल अन्य शेयरों में एनटीपीसी लिमिटेड (95.2% ऊपर), लार्सन एंड टुब्रो लिमिटेड (76.4% ऊपर), महिंद्रा एंड महिंद्रा लिमिटेड (70.3% ऊपर), पावर ग्रिड कॉर्पोरेशन ऑफ इंडिया लिमिटेड (66.2% ऊपर), सन फार्मास्युटिकल इंडस्ट्रीज लिमिटेड (64.7% ऊपर), भारती एयरटेल लिमिटेड (64.2% ऊपर), मारुति सुजुकी इंडिया लिमिटेड (53.5% ऊपर), और टाइटन कंपनी लिमिटेड (52.1% ऊपर) शामिल हैं। वित्त वर्ष 24 में दो पिछड़े शेयर हिंदुस्तान यूनिलीवर लिमिटेड (8.8% नीचे) और एचडीएफसी बैंक लिमिटेड (8.4% नीचे) थे। बाजार विशेषज्ञों का अनुमान है कि भारतीय वित्तीय बाजारों में आशावादी रुझान वित्त वर्ष 2025 में भी जारी रहेगा, जिसमें अस्थिरता मुख्य रूप से दुनिया भर में होने वाली घटनाओं के कारण होगी। ऐसा माना जाता है कि खुदरा निवेशकों, एचएनआई और डीआईआई सहित घरेलू निवेशकों की मजबूत भागीदारी से बाजारों को समर्थन मिलेगा। अब तक (28 मार्च) एफआईआई शुद्ध विक्रेता हैं, जिनका बहिर्गमन -16,200 करोड़ रुपये रहा है, जबकि डीआईआई शुद्ध खरीदार हैं, जिनका अंतर प्रवाह +2,20186 करोड़ रुपये से अधिक रहा है।

(सभी आंकड़े बीएसई, भारतीय रिजर्व बैंक, एनएसई की वेबसाइट के साथ दि.21-4-24 के इकोनॉमिक टाइम्स, दि.3-4-24 के मिंट तथा दि.3-4-24 के बिजनेस स्टैंडर्ड से साभार)

कब बचत करें और कब निवेश करें

बचत तथा निवेश के बारे में एक सामान्य प्रश्न उठता है, कि बचत करना चाहिए या निवेश करना चाहिए। इस सवाल का जवाब, विशेष वित्तीय स्थिति, लक्ष्यों और जोखिम सहनशीलता पर निर्भर करेगा। जब हम युवा होते हैं, तो हमारी आय और व्यय सीमित हो सकते हैं, लेकिन बचत और निवेश के बारे में सोचना शुरू करने के लिए कभी भी बहुत जल्दी नहीं होती और युवावस्था इसके लिए उचित समय है। वास्तव में, जल्दी शुरू करने से समय के साथ धन संचय करने में महत्वपूर्ण लाभ मिल सकता है। निवेश करने से भविष्य के लिए बचत जैसे दीर्घकालिक लक्ष्यों को पूरा करने में मदद मिल सकती है। युवा व्यक्ति के पास अधिक समय होता है, जिसका अर्थ है कि अधिक जोखिम उठाया जा सकता हैं और जोखिम भरी संपत्तियों में निवेश किया जा सकता हैं। भले ही अल्पावधि में नुकसान हो, लेकिन किसी व्यक्ति के पास लंबी अवधि के निवेश के सकारात्मक प्रभावों से उबरने और लाभ उठाने के लिए अधिक लचीलापन होता है। दूसरे शब्दों में, जल्दी और नियमित रूप से निवेश करके, चक्रवृद्धि की शक्ति का लाभ उठाया जा सकता हैं, जिसका अर्थ है कि निवेशित धन समय के साथ तेजी से बढ़ सकता है।

आयु बढ़ने के साथ ही समय कम बचता है और विशेषज्ञ, स्टॉक जैसी जोखिम भरी संपत्तियों से हटकर बॉन्ड और

नकदी जैसी अधिक रूढ़िवादी संपत्तियों में निवेश करने की सलाह देते हैं। ऐसा इसलिए है क्योंकि अगर आप रिटायर होने वाले हैं और बाजार में गिरावट आती है तो अल्पकालिक अस्थिरता एक संभावित जोखिम है। युवा व्यक्तियों के लिए भी, बचत करना आमतौर पर एक अच्छा विचार है। बचत का मतलब है अपने पैसे को एक सुरक्षित और कम जोखिम वाले खाते में रखना, जैसे कि बचत खाता, मनी मार्केट अकाउंट या जमा प्रमाणपत्र (सीडी)। इस तरह के बचत उत्पाद आमतौर पर कम रिटर्न देते हैं लेकिन वे कम जोखिम के साथ भी आते हैं। यदि आपको निकट भविष्य में अपने पैसे तक पहुँचने की आवश्यकता है और आप इसे खोने का जोखिम नहीं उठा सकते हैं तो वे एक अच्छा विकल्प हैं।

उद्देश्य: बचत और निवेश के बीच यह सबसे तेज अंतर है, निवेश के संदर्भ में, निवेश के लिए पूंजी उत्पन्न करने और तैयार करने के लिए बचत की जाती है। यही कारण है कि आपकी सभी बचत का निवेश न करने की सिफारिश की गई है। बचत आमतौर पर अल्पावधि होती है और कोई भी ज्यादा शोध किए बिना बचा सकता है। निवेश, दूसरी ओर धन निर्माण, घर खरीदने, शिक्षा के वित्तपोषण आदि जैसे बड़े लक्ष्यों को प्राप्त करने के लिए किया जाता है। निवेश में दीर्घकालिक प्रतिबद्धताओं और बाजार अनुसंधान की आवश्यकता हो सकती है। बचत केवल दुर्लभ परिस्थितियों में ही नीचे जाएगी, जबकि निवेश संभावित रूप से दोनों तरीकों से जा सकता हैं, अगर उचित परिश्रम के साथ बाजार अनुसंधान नहीं किया गया।

तरलता: बचत उपकरण आमतौर पर उच्च तरलता से जुड़े होते हैं, इसलिए बचत आपको जब जरूरत पड़े नकदी के लिए तैयार पहुँच के साथ प्रदान करती हैं। दूसरी ओर निवेश विभिन्न उपकरणों में तरलता का स्वरूप चलायमान हो सकता है। उदाहरण के लिए म्यूचुअल फंड या फिर शेयर बाज़ार में तरलता नहीं मिलती है, इसमें आवश्यकता पड़ने पर धन निकालना नुकसान दे सकता है। यही कारण है कि आपातकालीन धन का निवेश कभी नहीं किया जाना चाहिए।

जोखिम: बचत आमतौर पर बहुत कम या नगण्य जोखिम से जुड़ी होती है, जबकि निवेश उच्च जोखिम वाले उपकरणों और कम जोखिम वाले उपकरणों दोनों में किया जा सकता है। एफडी और बैंक खाते की शेष राशि जैसे उपकरण कभी भी गिरावट नहीं दिखाएंगे – आप हमेशा उन पर स्थिर ब्याज अर्जित करेंगे। हालांकि, निवेश कंपनी के प्रदर्शन, उस समय बाजार की स्थिति, अन्य उद्योगों का प्रदर्शन और अन्य आर्थिक और वित्तीय कारकों के अनुसार नीचे की ओर गति दिखा सकता है। यही कारण है कि निवेश आमतौर पर कुछ जोखिम के साथ सह-संबद्ध होते हैं, जबकि बचत "शून्य जोखिम" से जुड़ी होती है।

लाभ: यह निवेश तथा बचत के बीच अंतर का एक और महत्वपूर्ण बिंदु है आप आमतौर पर अपनी बचत पर ब्याज की केवल एक निश्चित और स्थिर राशि कमा सकते हैं। उदाहरण के लिए सावधि जमा पर विचार करें, जहां आप एक वर्ष से अधिक अपनी मूल राशि पर 4 -8% स्थिर ब्याज कमा सकते हैं। हालांकि, ये लाभ अक्सर मुद्रास्फीति जैसे कारकों के कारण बचत की दिशा में निर्देशित राशि के मूल्य को संरक्षित करने के लिए काम करते हैं। यही कारण है कि अन्य खर्चों को बढ़ावा देने के लिए बचत का उपयोग नहीं किया जा सकता। दूसरी ओर, यदि वे ऊपर की ओर गति दिखाते हैं तो निवेश में बहुत अधिक लाभ प्राप्त करने की क्षमता होती है। जैसा कि पहले उल्लेख किया गया है, निवेश उच्च जोखिम से जुड़ा हो सकता हैं। इन अंतरों को जानना एक निवेशक के लिए बहुत आवश्यक है, तभी इनकी लाभ हानि का अधिक सटीक रूप से विश्लेषण किया जा सकता है। तरलता की दृष्टि से बचत सुरक्षा नेट का गठन करती है जिसे आप आपातकाल के समय में वापस ले सकते हैं, निवेश में यह सुविधा उपलब्ध नहीं होती है। आपातकाल में यद्यपि निवेश को वापस लिया जा सकता है परन्तु उसमें अवसर लाभ खोने का खतरा रहता है।

कुछ लोग निवेश करने की बजाय बचत करना क्यों पसंद करते हैं?

कुछ लोग कई कारणों से निवेश करने के बजाय बचत करना पसंद कर सकते हैं। कुछ लोग अप्रत्याशित खर्चों या आपातकालीन स्थितियों के लिए बचत खाते में ज़्यादा पैसे रखने की सुरक्षा की भावना को पसंद करते हैं। कुछ लोगों के पास छुट्टी मनाने या घर के लिए डाउन पेमेंट जैसे कई अल्पकालिक वित्तीय लक्ष्य हो सकते हैं तथा उनका रुझान कम जोखिम वाले बचत खाते में धन रखने का होता हैं। इसके अलावा, कुछ लोगों के पास निवेश करने का ज्ञान या विशेषज्ञता नहीं हो सकती है या वे कम जोखिम सहन करने की क्षमता के कारण निवेश से जुड़े जोखिम के स्तर को लेकर सहज महसूस नहीं कर सकते हैं। अंत में, कुछ लोगों के पास अपने ज़रूरी खर्चों को पूरा करने के बाद निवेश करने के लिए पर्याप्त पैसा नहीं हो सकता है। अभ्यास में, सिद्धांत में बचत बनाम निवेश सिद्धांत रूप में उतना ही भिन्न होता है। उदाहरण के लिए, आपके खाते में बचत का पर्याप्त हिस्सा होना संभव है लेकिन फिर भी आपके दीर्घकालिक लक्ष्यों को पूरा करने में सक्षम नहीं है। जबकि बचत वित्तीय सुरक्षा प्रदान करेगी, लेकिन हो सकता है कि आप अपनी बचत के साथ अपने बच्चे की कॉलेज शिक्षा जैसी बड़ी और लंबी अवधि की आवश्यकताओं को पूरा न कर सकें। यही कारण है कि बचत और निवेश एक दूसरे के विकल्प नहीं है।

कितना पैसा बचाया जाना चाहिए और कितना निवेश किया जाना चाहिए?

निवेश की जाने वाली राशि और बचत की जाने वाली राशि व्यक्ति के व्यक्तिगत वित्तीय लक्ष्यों, जोखिम सहनशीलता और व्यक्तिगत परिस्थितियों पर निर्भर करती है। एक अच्छा नियम यह है कि आपातकालीन निधि में तीन से छह महीने के जीवन-यापन के खर्चों को पूरा करने के लिए पर्याप्त बचत करें; एक बचत खाता, जिसमें बिल जैसे अल्पकालिक दायित्वों को पूरा करने के लिए पर्याप्त राशि हो और फिर बाकी का निवेश करें। इस प्रकार निवेश की जाने वाली राशि और बचत की जाने वाली राशि उम्र, आय, मौजूदा ऋण और दीर्घकालिक वित्तीय लक्ष्यों जैसे कारकों के आधार पर अलग-अलग होगी। ऐसे कई कारण हैं जिनकी वजह से लोगों को निवेश करने में दिक्कत हो सकती है। एक आम कारण ज्ञान या अनुभव की कमी है, जो खराब निवेश निर्णयों को जन्म दे सकता है। इसके अतिरिक्त, भावनात्मक पूर्वाग्रह, जैसे कि डर या लालच, निवेशकों को खराब या तर्कहीन निर्णय लेने के लिए प्रेरित कर सकते हैं, जिसके परिणामस्वरूप नुकसान हो सकता है। सफल निवेश के लिए दीर्घकालिक दृष्टिकोण, अनुशासन और धैर्य की आवश्यकता होती है और बाजार में उतार-चढ़ाव के दौरान इस मार्ग पर बने रहना मुश्किल हो सकता है। वित्तीय विशेषज्ञ निवेश पोर्टफोलियो का बहुत अधिक हिस्सा नकदी में रखने की सलाह नहीं देते, क्योंकि इससे "नकदी खिंचाव" पैदा हो सकता है और आपके पोर्टफोलियो के संभावित रिटर्न में कमी आ सकती है।

एक योजना बनाने की आवश्यकता

अपनी ज़रूरतों और लक्ष्यों को पूरा करने के लिए पैसे बचाने के कई अलग-अलग तरीके हैं। कुछ उदाहरणों में स्वचालित बचत, सिक्कों की बचत, कूपन या रिफंड पर बैंकिंग बचत शामिल हैं। बस इस बारे में सोचें कि आपके लिए सबसे अच्छा क्या काम करता है। एक सुझाव यह है कि जब आपको पैसे मिलते हैं, तो समय के साथ पैसे बचाने की योजना बनाने के तरीके के रूप में, ''पहले खुद को भुगतान करें"। जब आप पहले खुद को भुगतान करते हैं, तो आप अन्य मदों पर खर्च करने से पहले बचत में एक राशि पहले रखते हैं। एक बार जब आप आपातकालीन जरूरतों को पूरा करने के लिए पैसे बचा लेते हैं, तो अपने पैसे को बढ़ाने के लिए अन्य बचत का निवेश करने पर विचार करें। अपने अल्पकालिक और दीर्घकालिक लक्ष्यों के बारे में सोचें। अपने दीर्घकालिक बचत लक्ष्यों के बारे में सोचने के लिए समय निकालना विशेष रूप से महत्वपूर्ण है क्योंकि बचाया गया पैसा समय के साथ बढ़ सकता है। यदि

आप इसे कई वर्षों तक बचत में रखते हैं तो आपकी बचत समय के साथ बढ़ सकती है।

दीर्घकालिक बचत के लाभ हैं। अपने फंड को और बढ़ाने के लिए दीर्घकालिक बचत का निवेश किया जा सकता है। अपने लक्ष्यों और जोखिम स्तरों के लिए उपयुक्त निवेश विकल्पों पर विचार करें। निवेश करके, आप यह तय कर रहे हैं कि अपना पैसा कहाँ लगाना है, यह कहाँ बढ़ेगा और आपको अपने लक्ष्यों को प्राप्त करने में मदद करने के लिए अतिरिक्त धन प्रदान करेगा। अपने भविष्य की योजना बनाते समय बचत और निवेश दोनों पर विचार करना महत्वपूर्ण है। पैसे बचाने से आपका पैसा सुरक्षित रहता है और ज़रूरत पड़ने पर आसानी से मिल जाता है। समय के साथ जल्दी निवेश करने से आपके पैसे का मूल्य बढ़ता है और चक्रवृद्धि ब्याज से लाभ मिलता है। याद रखें कि जल्दी निवेश करने से, चक्रवृद्धि ब्याज के साथ, देर से निवेश शुरू करने की तुलना में अधिक निवेश राशि मिल सकती है। निवेश में कुछ जोखिम उठाना शामिल है, इसलिए ऐसे निवेश चुनना ज़रूरी है जो आपके लक्ष्यों, जोखिम सहनशीलता और समय सीमा के साथ संरेखित हों। सामान्य तौर पर, जितना लंबा समय आप निवेश कर सकते हैं, उतना ही अधिक जोखिम आप उठा सकते हैं, क्योंकि आपके पास शेयर बाज़ार के उतार-चढ़ाव से निपटने के लिए अधिक समय होता है।

☯

DECLARATION FORM

The Editor,

Bank Quest,
Indian Institute of Banking & Finance, Kohinoor City, Commercial II,
Tower I, 2nd Floor, Kirol Road, Kurla (W), Mumbai - 400 070.

Dear Sir / Madam,

Re : Publication of my article

I have submitted an "_____" for publication at your quarterly journal Bank Quest.

In this connection this is to declare and undertake that the said article is my original work and that I am the author of the same. No part of the said article either infringes or violates any existing copyright or any rules there under.

Further, I hereby agree and undertake without any demur; to indemnify and keep the Institute (IIBF) indemnified against all actions, suits, proceedings, claims, demands, damages, legal fees and costs incurred by the Institute arising out of infringement of any copyright /IPR violation.

Yours faithfully,

(_____)

Author _____

Name : _____

Designation : _____

Organisation : _____

Address : _____

Tel. No. : _____

E-mail ID : _____

Signature : _____

Date : _____

BOOK REVIEW

Name of the Book: Banking Beyond Borders
Author: Shri Mohan Vasant Tanksale, Former Chairman, Central Bank of India and Executive Director, Punjab National Bank
Publisher: Indie Press
Year: 2024
Pages: 148
Price: Rs. 299/-

Reviewed by: Dr. Brinda Jagirdar, Former Chief Economist, State Bank of India.

There is always a map for those looking for directions and for those looking to understand Indian banking, Shri Mohan Vasant Tanksale's book "Banking Beyond Borders" is a ready reckoner. The book makes compelling reading with its easy, flowing style and many actionable points that can be applied to situations even in today's banking scenario. Readers will find the book unputdownable especially for those who want to walk down memory lane, but also Gen Z who cannot imagine life without smartphones and spreadsheets. The book takes you along a fascinating journey starting from his first job as a clerk at the Central Bank of India, a short stint at State Bank of India, a successful career at Union Bank of India, later serving as Executive Director at Punjab National Bank and Chairman at Central Bank of India and finally as Chief Executive, Indian Banks' Association.

The author gives a ringside view of developments as he successfully captures the transformation in banking over the last five decades – from class banking to mass banking, from branch customer to bank customer and from manual banking to core banking. The book is a testament to his learnings from successful and spiritually fulfilling innings in banking, grassroots wisdom and old-school reflections which remain relevant even in today's age of digital banking.

The book makes compelling reading for those who want to understand the practical side of banking. The author has clearly explained important concepts – cost-income ratio, price to book value, balance sheet analysis, various aspects of lending, the importance of the composition of deposits, trade finance, risk management, foreign exchange, credit assessment and follow-up, and Non-Performing Assets (NPAs) management. The book has something for everyone. Students and the lay public can learn about the nitty gritty of banking. Mr. Tanksale equips new entrants and mid-career bankers to face challenges and advises them to pay close attention to detail. For Senior Officers and Top Executives, his advice, among others, is to take a 360-degree view of the environment, understand risk, keep close track of customers, empathize with juniors, encourage and empower them while demanding performance.

Interestingly, the book does not look at banking in isolation but as a very important tool in the development and progress of the Indian economy. Mr. Tanksale feels bankers are not merely lenders but partners in business and as a partner, the banker must know about the customer's

business be it agriculture, industry or services. His advice to bankers is to look beyond profit and consider financial inclusion as a contribution to society: "The role of banking in our society goes beyond deposit mobilization and lending… it is the lifeline of any economy and therefore, no matter what strides we make in our economy or industry, true progress can be seen only when we meet the objectives of financial inclusion".

Mr. Tanksale's success as a banker is underpinned by values and ethics and his firm belief that good ethics is good business. He followed instructions and policies in letter and spirit and remained undaunted in the face of challenges. Sharing his mantra for success, Mr. Tanksale says he converted every opportunity into business by taking it on as a challenge and succeeding. As one continues reading the book, one uncovers the secret of his success: his self-confidence, his faith in God, constant study and preparation, taking every opportunity to learn and acquire new skills, always being a team player who won the respect and admiration of his juniors, peers and confidence of his seniors. Throughout the book, the author freely shares his learnings and advice to aspiring and career bankers. Some gems that stand out for me: Do not use a dagger when you can kill with a smile. A leader must create leaders, not followers. Think like a CEO. KYC is not only Know Your Customer but Know Your Competition. Know Your Borrower (KYB) but also Know Your Borrower's Customer (KYBC). Importantly, Know Your Own Bank (KYOB).

Coming from a non-technical and non-banking background, he mastered both and applied the learnings successfully in his career, rising to the topmost position in banking. Not surprisingly, Mr. Tanksale is most at ease dealing with technology and customers – two essential ingredients for success in banking. As he says "The moment we have a product that fits the customer's needs and the technology to fulfil that need, it is a win-win situation." Technology has made life easier for bankers today, as "besides due diligence, even monitoring and recovery has now been enabled by technology". Of course, technology and Artificial Intelligence (AI) will pose a big challenge. Still, banks can use this as an opportunity and leverage customer's data to cross-sell products, customize products as per customer's preference and more importantly, extend credit to New to existing Bank customers.

The author is bang on when he says the future of banking lies in agribusiness, small businesses and financial inclusion taking banking to the last mile customers across geographies, standing out in the competition by reinventing themselves, improving productivity, competing against mutual funds to raise low-cost deposits, besides AI, cyber security and Account Aggregation. Given his knowledge and involvement in technology, his deep understanding of banking, Society for Worldwide Interbank Financial Telecommunications (SWIFT), Unified Payments Interface (UPI), digitization, one would like the author to bring out a sequel focusing on technology, its pitfalls and how banks can safeguard themselves and their customers. For now, Banking Beyond Borders is a good place to start.

Bank Quest – Guidelines for Manuscript Submission

Contributing articles to the Bank Quest : (English/ Hindi)

Original works by the author or authors should be submitted to Bank Quest. Only unpublished articles that have not been submitted for publication elsewhere will be considered for publication. Papers that are submitted to the Bank Quest for publication should not be under review at other journals.

Articles should be sent to: editor@iibf.org.in

Objectives:

The primary objective of Bank Quest is to present the theory, practice, analysis, views and research findings on issues/developments, which have relevance for current and future of banking and finance industry.

The aim is to provide a platform for Continuing Professional Development (CPD) of the members of the Institute and also to create a space for the academics in disseminating original research outcomes and innovative knowledge in the field of banking and finance.

Guidelines for manuscript submission

Each article submitted to Bank Quest is initially assessed by the Editor for general suitability. It may then be subjected to a review process by the experts in the field. On the basis of the feedback of the reviewer the article will be either accepted or rejected. If minor corrections are suggested, then the contributor will be asked to rectify the anomalies pointed by the reviewer and submit and if it's found satisfied the article will be considered for publication. The Editor has the discretion to vary this process.

The articles for Bank Quest should have a uniform template in the form of a title focussing on the core of the work done, an abstract, introduction and background, statement of the problem, review of literature, theoretical or conceptual framework, objectives, methodology, hypothesis if any, analyses and discussion, Suggestions and policy recommendations, conclusion, end notes if any and references.

Authors should carefully note the following before submitting any articles:

Format: The article, should be submitted in MS Word, Times New Roman, Font Size 12 with 1½ line spacing. The primary heading should be in capitalized form (Uppercase) and boldface. The sub-headings should be in title - case capitalization (first letter of each word in capital), in bold, and should be italicized.

Manuscripts should be prepared using APA style. For detailed information, refer to the Publication Manual of the American Psychological Association (7th ed.), http://apastyle.org

Word Length: The research articles may be in the range of 5000 to 6000 words in length. However, the contents of the article should justify the words.

The other articles may range between 2000 to 3000 words depending on the subject, coverage and quality.

Author's Profile: The cover page of the article should include full name, designation, name of organization, telephone and fax numbers, and e-mail address or last position held in case of retired persons. The author's name or affiliations should not appear anywhere else in the body of the manuscript. The actual paper should commence from the second page containing the title followed by the Abstract, Keywords, and the main paper.

Title: A title of, preferably, fifteen words or less should be provided.

Abstract: The abstract should be clear and provide an excellent summary of each article's content. It should briefly describe the objectives, explain how the study was done, and summarize the key results. The Abstract should be written in past tense and should not be more than 250 words. Avoid the use of abbreviations and references in the abstract. The Abstract should be followed by relevant keywords.

Figures, charts and diagrams: Essential figures, charts and diagrams should be referred to as 'Figures' and they should be numbered consecutively using Arabic numerals. Each figure and diagram should have brief title. Diagrams should be kept as simple as possible. Figures, charts and diagrams should be provided in the text and should also be provided in original formats.

Tables: Use of tables, wherever essential, should be done within the article, also it should be printed or typed on a separate sheet of paper and numbered consecutively using Arabic numerals (e.g. Table-1) and contain a brief title. Tables should be numbered consecutively as Table 1, Table 2, Table 3, and so on (and not as Table 1.1, Table 1.2, Table 1.3, and so on). The title of the table should be placed above the table. The source should be indicated at the bottom.

Picture/photos/illustrations: The reproduction of any photos, illustration or drawings will be at the Editor's discretion. Sources should be explicitly acknowledged by way of footnote, all computer-generated pictures should be clear and sharp.

Emphasis: Words to be emphasised should be limited in number and italicised. Capital letters should be used only at the start of the sentences or for proper names.

References: References should be included at the end of the paper. All the references should be cited in the body of the text. References and citations should be complete in all respects and arranged in alphabetical order. Authors are requested to include only a list of cited References and not a Bibliography. Reference to a citation in the text should be made by means of the author's name followed by the year of publication in parenthesis. The references must follow the style guide of the American Psychological Association (APA) (7th edition). Example;

Tobin, J. (1958): Liquidity Preference as Behaviour Towards Risk, Review of Economic Studies, Vol.25, pp.65-86.

Tobin: J. (1971): Essays in Economics, Vol. 1, Macroeconomics, Amsterdam: North Holland

Shrotryia,V.K., and Kalra, H.(2022). Herding in the Crypto Market: A Diagnosis of Heavy Distribution Tails. Review of Behavioural Finance, 14(5), 566- 587.

Footnotes & Endnote: Footnotes, italics, and quotation marks should be kept to the minimum. All notes must be serially numbered. These may be given at the end of the Paper or on every page as endnotes.

Contributors whose papers are accepted or rejected will be informed by email only.

Copyright: It is important that authors submitting articles should declare that the work is original and does not infringe on any existing copyright. He/ she should undertake to indemnify the Institute against any breach of such warranty and consequential financial and other damages. Copyright of published article will vest with publisher (Institute).

The Editor: Bank Quest

Indian Institute of Banking and Finance

Kohinoor city Commercial II, Tower 1,

Kirol Road, Kurla West, Mumbai 400 070

IIBF - PUBLICATION LIST

Sr. No	Examination	Medium	Name of the Book	Edition	Published by	Price (Rs.)
21	Diploma in Banking Technology	English	IT Data Commmunication and Electronic Banking	2017	M/s Macmillan Education India Pvt. Ltd.	435/-
22	Diploma in Banking Technology	English	Security in Electronic Banking	2017	M/s Macmillan Education India Pvt. Ltd.	314/-
23	Diploma in Co-Operative Banking	English	Cooperative Banking - Principles, Laws & Practices	2017	M/s Macmillan Education India Pvt. Ltd.	315/-
24	Diploma in Co-Operative Banking	English	Management and Operations of Co-operative Banks	2017	M/s Macmillan Education India Pvt. Ltd.	445/-
25	Diploma in International Banking	English	International Banking - Legal & Regulatory Aspects	2017	M/s Macmillan Education India Pvt. Ltd.	245/-
26	Diploma in International Banking	English	International Corporate Finance	2017	M/s Macmillan Education India Pvt. Ltd.	290/-
27	Diploma in International Banking	English	International Banking - Operations	2017	M/s Macmillan Education India Pvt. Ltd.	285/-
28	Diploma in Retail Banking	English	Retail Assets Products & Other Related Services	2017	M/s Macmillan Education India Pvt. Ltd.	360/-
29	Diploma in Retail Banking	English	Retail Liability Products & Other Related Services	2017	M/s Macmillan Education India Pvt. Ltd.	380/-
30	Certificate Course	English	Foreign Exchange Facilities for Individuals	2025	M/s Macmillan Education India Pvt. Ltd.	730/-
31	Certificate Course	English	Micro Finance	2014	M/s Macmillan Education India Pvt. Ltd.	365/-
32	Certificate Course	English	Prevention of Cyber Crimes & Fraud Management	2017	M/s Macmillan Education India Pvt. Ltd.	245/-
33	Strategic Management Certificate Examinations	English	Strategic Management & Innovations in Banking	2021	M/s Macmillan Education India Pvt. Ltd.	450/-
34	Certified Credit Professional	English	Bankers' Handbook on Credit Management	2023	M/s Taxmann Publications Pvt. Ltd.	1300/-
35	Certified Accounting & Audit Professional	English	Bankers' Handbook on Accounting	2023	M/s Taxmann Publications Pvt. Ltd.	930/-
36	Certified Accounting & Audit Professional	English	Bankers' Handbook on Auditing	2023	M/s Taxmann Publications Pvt. Ltd.	1075/-
37	Certificate Course in Digital Banking	English	Digital Banking	2024	M/s Taxmann Publications Pvt. Ltd.	775/-
38	Other Publications	English	Banking & Finance Year Book	2024	M/s Taxmann Publications Pvt. Ltd.	545/-
39	Business Correspondents/ Facilitators	English	Inclusive Banking Through Business Correspondents (Basic Course)	2024	M/s Taxmann Publications Pvt. Ltd.	375/-
40	Business Correspondents/ Facilitators	Marathi	Inclusive Banking Through Business Correspondents (Basic Course)	2024	M/s Taxmann Publications Pvt. Ltd.	490/-

IIBF - PUBLICATION LIST

Sr. No	Examination	Medium	Name of the Book	Edition	Published by	Price (Rs.)
41	Business Correspondents/ Facilitators	Hindi	Inclusive Banking Through Business Correspondents (Basic Course)	2024	M/s Taxmann Publications Pvt. Ltd.	485/-
42	Business Correspondents/ Facilitators	Bengali	Inclusive Banking Through Business Correspondents (Basic Course)	2024	M/s Taxmann Publications Pvt. Ltd.	425/-
43	Business Correspondents/ Facilitators	Oriya	Inclusive Banking Through Business Correspondents (Basic Course)	2024	M/s Taxmann Publications Pvt. Ltd.	455/-
44	Business Correspondents/ Facilitators	Assamese	Inclusive Banking Through Business Correspondents (Basic Course)	2024	M/s Taxmann Publications Pvt. Ltd.	445/-
45	Business Correspondents/ Facilitators	Gujarati	Inclusive Banking Through Business Correspondents (Basic Course)	2024	M/s Taxmann Publications Pvt. Ltd.	480/-
46	Business Correspondents/ Facilitators	Malayalam	Inclusive Banking Through Business Correspondents (Basic Course)	2024	M/s Taxmann Publications Pvt. Ltd.	665/-
47	Business Correspondents/ Facilitators	Tamil	Inclusive Banking Through Business Correspondents (Basic Course)	2024	M/s Taxmann Publications Pvt. Ltd.	600/-
48	Business Correspondents/ Facilitators	Kanada	Inclusive Banking Through Business Correspondents (Basic Course)	2024	M/s Taxmann Publications Pvt. Ltd.	435/-
49	Business Correspondents/ Facilitators	Telugu	Inclusive Banking Through Business Correspondents (Basic Course)	2024	M/s Taxmann Publications Pvt. Ltd.	500/-
50	Business Correspondents/ Facilitators	English	Inclusive Banking Through Business Correspondents (Advanced Course)	2024	M/s Taxmann Publications Pvt. Ltd.	545/-
51	Business Correspondents/ Facilitators	Marathi	Inclusive Banking Through Business Correspondents (Advanced Course)	2024	M/s Taxmann Publications Pvt. Ltd.	735/-
52	Business Correspondents/ Facilitators	Hindi	Inclusive Banking Through Business Correspondents (Advanced Course)	2024	M/s Taxmann Publications Pvt. Ltd.	655/-
53	Business Correspondents/ Facilitators	Bengali	Inclusive Banking Through Business Correspondents (Advanced Course)	2024	M/s Taxmann Publications Pvt. Ltd.	625/-
54	Business Correspondents/ Facilitators	Oriya	Inclusive Banking Through Business Correspondents (Advanced Course)	2024	M/s Taxmann Publications Pvt. Ltd.	660/-
55	Business Correspondents/ Facilitators	Assamese	Inclusive Banking Through Business Correspondents (Advanced Course)	2024	M/s Taxmann Publications Pvt. Ltd.	635/-

IIBF - PUBLICATION LIST

Sr. No	Examination	Medium	Name of the Book	Edition	Published by	Price (Rs.)
56	Business Correspondents/ Facilitators	Gujarati	Inclusive Banking Through Business Correspondents (Advanced Course)	2024	M/s Taxmann Publications Pvt. Ltd.	680/-
57	Business Correspondents/ Facilitators	Malayalam	Inclusive Banking Through Business Correspondents (Advanced Course)	2024	M/s Taxmann Publications Pvt. Ltd.	870/-
58	Business Correspondents/ Facilitators	Tamil	Inclusive Banking Through Business Correspondents (Advanced Course)	2024	M/s Taxmann Publications Pvt. Ltd.	785/-
59	Business Correspondents/ Facilitators	Kanada	Inclusive Banking Through Business Correspondents (Advanced Course)	2024	M/s Taxmann Publications Pvt Ltd	690/-
60	Business Correspondents/ Facilitators	Telugu	Inclusive Banking Through Business Correspondents (Advanced Course)	2024	M/s Taxmann Publications Pvt Ltd	660/-
61	Certified Banking Compliance Professional	English	Compliance in Banks	2017	M/s Taxmann Publications Pvt. Ltd.	1135/-
62	Certificate Course in Ethics in Banking	English	Ethics in Banking	2024	M/s Taxmann Publications Pvt. Ltd.	980/-
63	Debt Recovery Agent Examination	Marathi	Handbook On Debt Recovery	2023	M/s Taxmann Publications Pvt. Ltd.	790/-
64	Debt Recovery Agent Examination	Tamil	Handbook On Debt Recovery	2023	M/s Taxmann Publications Pvt. Ltd.	860/-
65	Debt Recovery Agent Examination	English	Handbook On Debt Recovery	2023	M/s Taxmann Publications Pvt. Ltd.	540/-
66	Debt Recovery Agent Examination	Telugu	Handbook On Debt Recovery	2023	M/s Taxmann Publications Pvt. Ltd.	695/-
67	Debt Recovery Agent Examination	Gujarati	Handbook On Debt Recovery	2023	M/s Taxmann Publications Pvt. Ltd.	715/-
68	Debt Recovery Agent Examination	Hindi	Handbook On Debt Recovery	2023	M/s Taxmann Publications Pvt. Ltd.	790/-
69	Debt Recovery Agent Examination	Oriya	Handbook On Debt Recovery	2024	M/s Taxmann Publications Pvt. Ltd.	560/-
70	Debt Recovery Agent Examination	Assamese	Handbook On Debt Recovery	2024	M/s Taxmann Publications Pvt. Ltd.	580/-
71	Debt Recovery Agent Examination	Kannada	Handbook On Debt Recovery	2024	M/s Taxmann Publications Pvt. Ltd.	575/-
72	Debt Recovery Agent Examination	Malayalam	Handbook On Debt Recovery	2024	M/s Taxmann Publications Pvt. Ltd.	570/-

IIBF - PUBLICATION LIST

Sr. No	Examination	Medium	Name of the Book	Edition	Published by	Price (Rs.)
73	Debt Recovery Agent Examination	Bengali	Handbook On Debt Recovery	2024	M/s Taxmann Publications Pvt. Ltd.	570/-
74	Certified Information System Banker	English	Information System For Banks	2017	M/s Taxmann Publications Pvt. Ltd.	645/-
75	Certificate Course on Resolution of Stressed Assets With Special Emphasis on Insolvency and Bankruptcy Code, 2016 for Bankers	English	Resolution of Stressed Assets With Special Emphasis on Insolvency and Bankruptcy Code, 2016 for Bankers	2025	M/s Taxmann Publications Pvt. Ltd.	630/-
76	Certificate in International Trade Finance	English	International Trade Finance	2025	M/s Taxmann Publications Pvt. Ltd.	625/-
77	Advanced Wealth Management	English	Introduction To Financial Planning	2017	M/s Taxmann Publications Pvt. Ltd.	390/-
78	Advanced Wealth Management	English	Investment Planing Tax Planing Estate Planing	2017	M/s Taxmann Publications Pvt. Ltd.	420/-
79	Certificate Examination in IT Security	English	IT security	2024	M/s Taxmann Publications Pvt. Ltd.	435/-
80	Certificate course on MSME	English	Micro Small And Medium Enterprises	2022	M/s Taxmann Publications Pvt. Ltd.	750/-
81	Certificate Course for Non-Banking Financial Companies	English	Non Banking Financial Companies	2017	M/s Taxmann Publications Pvt. Ltd.	615/-
82	Advanced Wealth Management	English	Risk Analysis, Insurance & Retirement Planning	2017	M/s Taxmann Publications Pvt. Ltd.	240/-
83	Certificate Examination For Small Finance Banks	English	Small Finance Banks	2018	M/s Taxmann Publications Pvt. Ltd.	865/-
84	Certified Examination for Emerging Technologies	English	Emerging Technologies	2024	M/s Taxmann Publications Pvt Ltd	730/-
85	Diploma in Treasury, investment and Risk Management	English	Treasury, Investment and Risk Management	2017	M/s Taxmann Publications Pvt Ltd	730/-
86	Basics of Microfinance: Foundation Course	English	Basics of Microfinance: Foundation Course	2024	M/s Macmillan Education India Pvt. Ltd.	730/-
87	Other Publications	English	Shri R.K. Talwar Memorial Lectures (2007-2021)	2022	M/s Taxmann Publications Pvt. Ltd.	400/-

Printed at Onlooker Press: M.: 9321927244 Tel.: 45222939, 45223544, 31509862