



# Spotlight on Internal (office) accounts!

KPMG. Make the Difference.



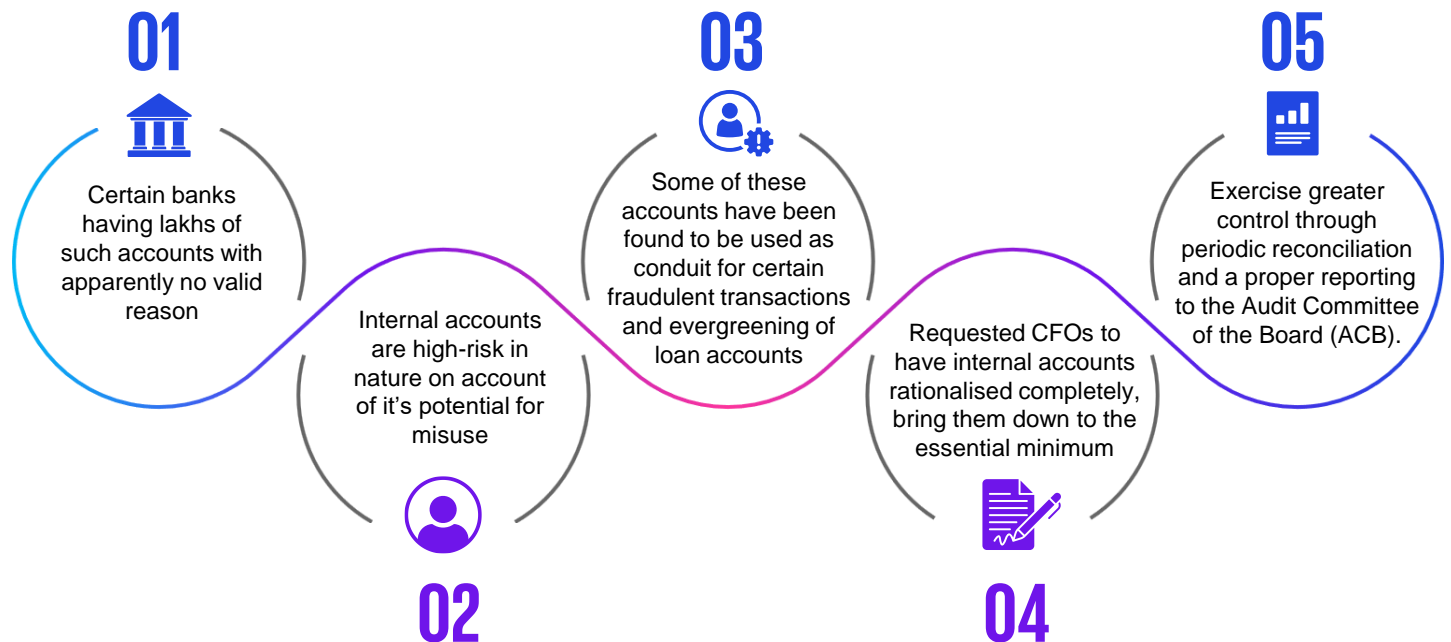
## I. Background

The expansion and complexity of financial activities undertaken by banks have underscored the necessity of maintaining a robust system to manage internal (office) accounts. These accounts are the foundation of banking services and internal financial activities. The Reserve Bank of India (RBI) has emphasised on an increasing need of implementing controls over opening and operations of internal (office) accounts, supported by necessary oversight, checks and audits. By scrutinising and strengthening the control framework on internal (office)

accounts, banks can ensure seamless and resilient operations and uphold a high level of financial integrity and transparency.

During a conference of Statutory Auditors and Chief Financial Officers (CFOs) of commercial banks and All India Financial Institutions organised by the RBI on 9 July 2024, Mr. Swaminathan Janakiraman, Deputy Governor, remarked specifically on usage of 'internal accounts' by the banks.

As per the news articles published<sup>1</sup>, five key points related to 'internal accounts' usage by banks as highlighted during the conference were as follows:



1. CFOs, auditors must follow regulations in letter and spirit says RBI, The Economic Times, Joel Rebello, July 10, 2024  
Lenders should rationalise "internal accounts": RBI Dy Guv Swaminathan, The Hindu BusinessLine, BL Mumbai Bureau, July 9, 2024

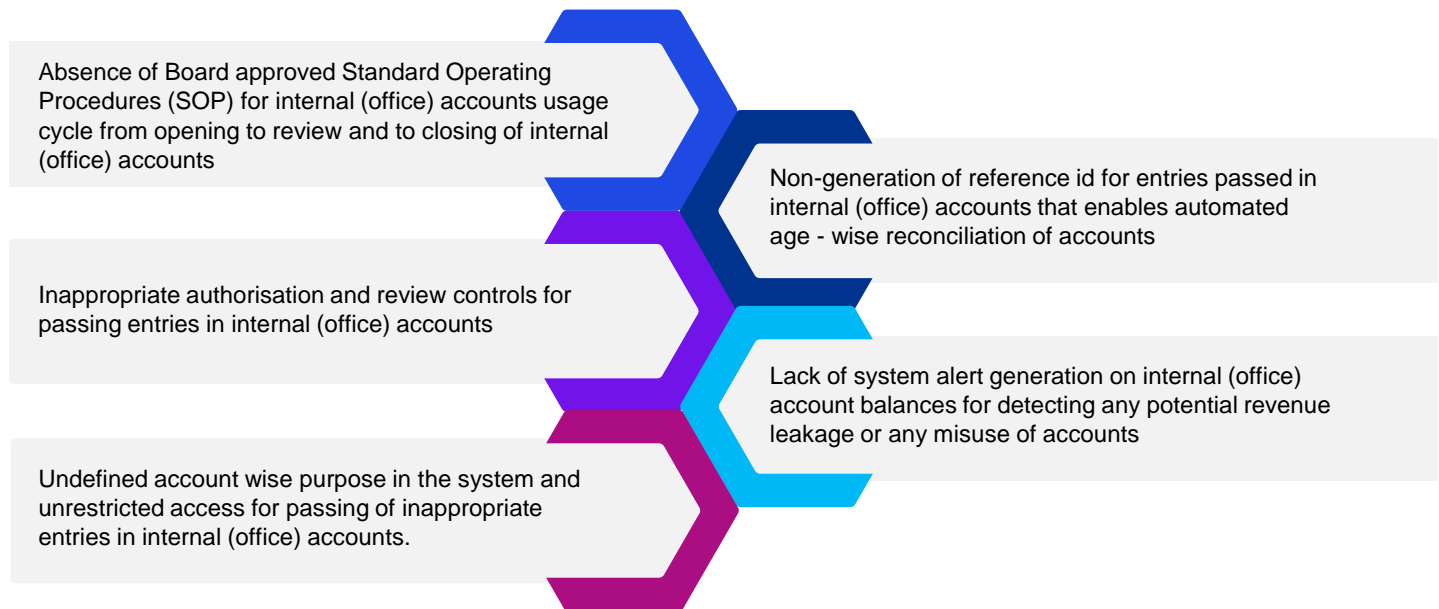
## II. What are 'internal (office) accounts' in banks?

'Internal (office) accounts' are accounts used solely for the purpose of transfers within the various business units of a bank and are distinct from customer accounts. The key purposes for operation of internal (office) accounts within a bank are cash management, inter branch reconciliations, management of income and expenses, movement of funds in treasury et al. In a typical banking scenario, access to these accounts is allocated to employees of respective branches/departments basis their usage needs, ownership

roles, and delegated authority. Nonetheless, the Finance and Accounts (F&A) department commonly serves as the key custodian of these internal (office) accounts. We see that the F&A department is involved in various aspects including (but not limited to) opening and setting up, operations, overseeing the reconciliation process, reporting of balances/long outstanding dues and closure of internal (office) accounts.

## III. RBI's concern on operations of internal (office) accounts

RBI had issued a circular to the all scheduled commercial banks/small finance banks/payment banks (DBS.CO.PPD./472/11.01.005/2019-20) dated 17 July 2019 on "un-authorized operation of internal / office accounts" and showed its concern relating to the following aspects:



These practices would lead to operational inefficiencies, account and record manipulation and financial losses. Banks are required to ensure and exercise appropriate checks and controls and implement corrective measures to prevent unauthorised operations in internal (office) accounts.



## IV. What are the common challenges of internal (office) accounts?

Basis our extensive experience on assisting financial institutions in reviewing internal (office) accounts, the key issues in management of internal (office) accounts and indicative actions the management may take are summarised below:

Sr No.	Key issues	Indicative actions
01	<b>Unclear purpose and ownership definition –</b> Lack of clarity or ambiguity in defining the specific purpose for which internal (office) accounts are required leading to risk of misinterpretation and duplication of accounts. Further, no clear definition of account ownership leads to lack of accountability.	<ul style="list-style-type: none"> <li>a. Define clear policies indicating purpose of internal (office) accounts</li> <li>b. Assign clear ownership and accountability for each account to specific departments and employees</li> </ul>
02	<b>Unauthorised setup and access to accounts –</b> Setting up of accounts not in line or beyond the purpose or attributes defined and lack of access rights controls leads to risk of unauthorised accesses and misuse of funds	<ul style="list-style-type: none"> <li>a. Implement a robust governance framework that outlines processes and procedures for setting up of accounts and access rights provisioning to users of internal (office) accounts</li> <li>b. Establish a clear approval matrix for creation, operation, and closure of internal (office) accounts</li> </ul>
03	<b>Inadequate control on usage of accounts –</b> Inadequate system level transaction controls (including manual intervention) leads to risk of posting transactions beyond the defined purpose of accounts	<ul style="list-style-type: none"> <li>a. Evaluate operational risks and consider implementing technological solutions for operating internal (office) accounts (including predefined attributes) and minimisation of manual discretion/ intervention</li> <li>b. Provide limited access rights strictly on 'need to know' and 'need to do' basis</li> <li>c. Optimise internal controls in the system for mitigating operational risks versus improving efficiency of internal (office) account operations</li> </ul>
04	<b>Lack of independent monitoring –</b> Absence or ineffective mechanism for periodic review and monitoring of transactions and balances in internal (office) accounts leading to risk of unreconciled long outstanding entries	<ul style="list-style-type: none"> <li>a. Implement a rule-based transaction monitoring system for alert generation and disambiguation along with monitoring of unreconciled account balances</li> <li>b. Internal audit to assess the need for continuity of internal (office) accounts and obtain confirmation on their ownership, at a predefined periodicity</li> </ul>
05	<b>Inadequate reporting mechanism –</b> Lack of periodic review of internal (office) accounts and reporting to senior management or board leading to lack of transparency and ineffective decision making.	<ul style="list-style-type: none"> <li>a. Conduct periodic reviews for operations of internal (office) accounts and publish MIS reports and reporting significant aspects to relevant management and committees of the Board including ACB.</li> </ul>

## V. What immediate actions can banks take?

Unauthorised usage of internal (office) accounts poses significant risks ranging from regulatory non-compliance to financial losses and reputational damage. To evaluate the existing control framework and mitigating the risks associated with operations of internal (office) accounts, the banks may consider undertaking the following steps:

- a. Conduct diagnostic review across the operating landscape of internal (office) accounts to include the following aspects:
  - Comprehensive review of office account framework by considering elements of purpose, ownership, lifecycle, usage and attributes of internal (office) accounts
  - Assess the User Access Management (UAM) system implemented for internal (office) accounts including access rights provisioning and existence of control framework for account operations
  - Evaluate the bank's compliance with regulatory requirements, industry standards and internal policies governing the use and management of internal (office) accounts
  - Evaluate the adequacy of systems implemented for reconciliation and monitoring for spurt management and transaction monitoring, alert generation, and resolution mechanism

- Analyse the Non-Performing Assets (NPA) identification criteria and provisioning mechanism
  - Review the coverage and inclusions of management reporting for internal (office) accounts.
- b. Basis identification of gaps across the abovementioned categories, conduct detailed review and analysis on datasets including transaction level review for rationalisation of existing internal (office) accounts
  - c. Ascertain remediation steps and evaluate implementation of enhanced mechanisms to mitigate risks, optimise the control framework and operations of internal (office) accounts and achieve compliance with regulatory guidelines and industry best practices
  - d. Conduct post implementation reviews to evaluate the implementation and effectiveness of remediation action plan and enhanced control mechanisms.

Our team will be happy to delve deeper into the nuances and address specific questions or challenges.

For follow-up conversations, please feel free in writing to Anoop Sharma by [clicking here](#).

KPMG in India would like to thank Dixita Bhalawat, Tanmay Rane, Nisha Fernandes and Khushi Kansara for their contribution.

## KPMG in India contacts:

### Manoj Kumar Vijai

Office Managing Partner – Mumbai  
and Head – Risk Advisory  
T: +91 98926 00654  
E: mkumar@kpmg.com

### Jagvinder S. Brar

Partner and Head  
Forensic Services and F-Tech  
T: +91 97169 09339  
E: jsbrar@kpmg.com

### Suveer Khanna

Partner and Head  
Forensic Investigations  
T: +91 96196 32131  
E: skhanna@kpmg.com

### Anoop Sharma

Director  
Forensic Services  
T: +91 98334 83595  
E: anoopsharma@kpmg.com

[kpmg.com/in](https://kpmg.com/in)

Follow us on:

[kpmg.com/in/socialmedia](https://kpmg.com/in/socialmedia)



The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

© 2024 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organisation.

This document is for e-communication only. (016\_FLY0724\_KK)