Revenue Assurance and Fraud Management (RAFM) Survey Report

August 2025

kpmg.com/in

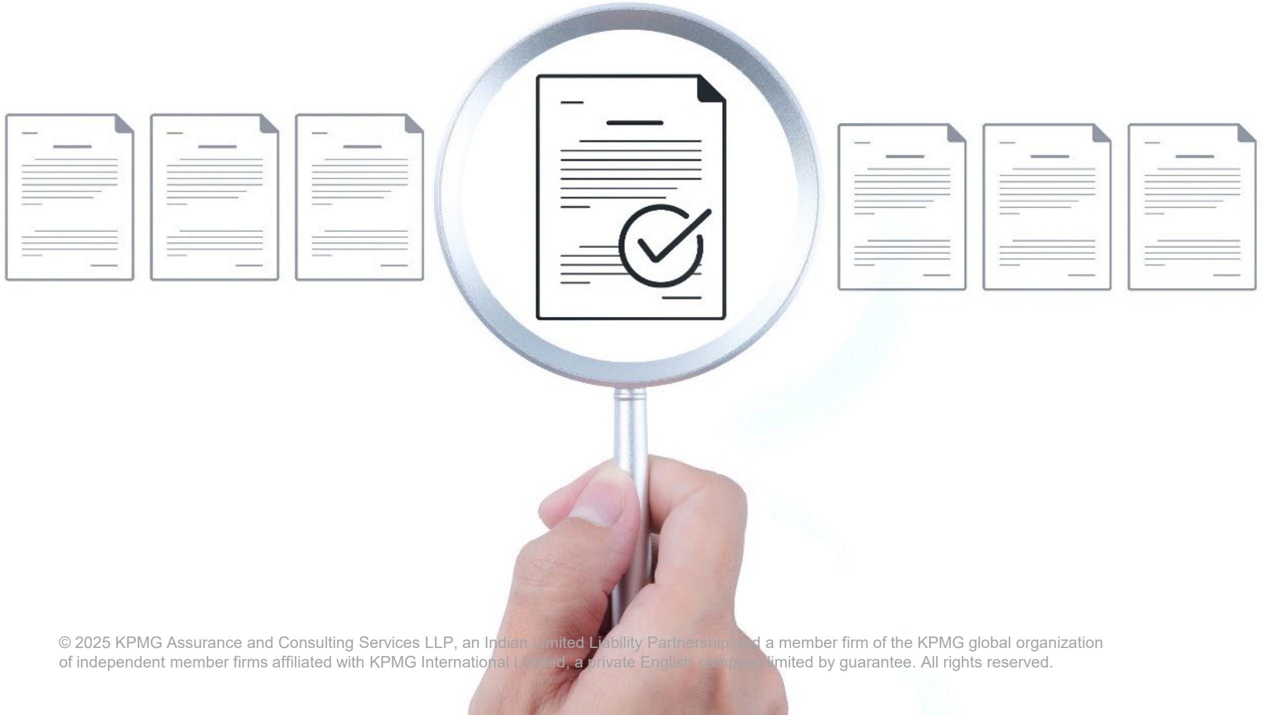
KPMG. Make the Difference.

Table of contents

Foreword

KPMG in India conducted a detailed RAFM Survey to evaluate the evolving maturity of Revenue Assurance and Fraud Management (RAFM) functions within organisations, with a focus on how these traditional control-centric domains are transforming in response to digital acceleration, advanced technology adoption, and shifting business priorities. The survey was driven by the need to understand how telecom enterprises and adjacent industries are adapting their assurance mechanisms in an increasingly automated, data-rich, and risk-prone environment.

Over the past decade, RAFM has shifted from being a reactive gatekeeper for revenue leakage to an intelligence-led framework that must proactively assure not only revenues but also broader value flows and operational integrity. This survey sought to capture that shift and examine the extent to which organisations are embracing this evolution in their internal governance, systems, technology investments, and strategic outlook.



"Generative AI is gaining traction in Business Assurance, but Agentic AI is emerging fast. Within the next 18 months, Telcos and MVNOs worldwide will start using Agentic AI to enhance decision-making and human-agent collaboration—freeing up time to scale into more advanced assurance areas."

Purushothaman KG
Partner – Advisory
Head - Technology Transformation & Telecommunication
KPMG in India

At a glance

KPMG's RAFM survey insights at a glance…

Organisations increasingly see AI-enabled RAFM as a strategic asset

47% organisations **assess risks annually** and have stressed upon **the importance of AI in real time risk monitoring**

40% organisations **rate risk coverage as "good"** while harping on the **importance of continual maturity improvement with AI**

Ramping up investments in AI-driven RAFM transformation

30% have **apportioned budgets for AI, ML and RPA driven Business Assurance (BA) transformation**

76% believe that **AI will drive transformation in RAFM operations** despite current hurdles

Assessment of the current control environment for AI enabled deployments will be key to a transformative journey

14% are currently able to derive **full scale value from their existing AI, ML and RPA tools**

26% have realized the importance of **AI enabled intelligence for fraud threat preparedness**

42% have **approved plans on improving their analytics pipeline for RAFM**

53% agree on the fact that **automation of the FM environment is seeing growth**

Awareness of BA challenges drives smarter prioritization

53% have identified **partial control testing as a major challenge** in the current BA environment

36% identify that there are **budget limitations in BA areas** such as regulatory reporting, new product development & asset assurance

Transformative BA success depends on matching the right tech and partner to each use case.

72% have identified use-cases of **application of block-chain for billing integrity checks**

35% **Are utilizing RPA for workflow automations** such as alarms and exception closure

30% have **ensured data lake readiness for ML deployments**

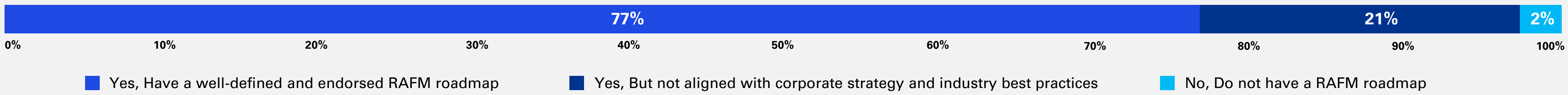
48% have **cited vendor technology dependencies** as a major bottleneck for BA transformation

Survey findings

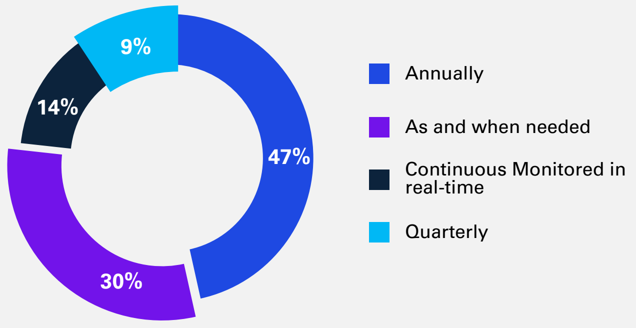
Strategic alignment & governance

Survey insights into the strategic coherence, governance maturity, and operational robustness of the RAFM function across organisations, including roadmap alignment, risk review cadence, control frameworks, and budgetary adequacy.

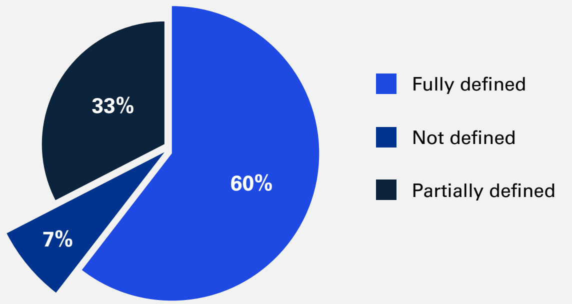
Distribution of RAFM roadmap alignment among organisations



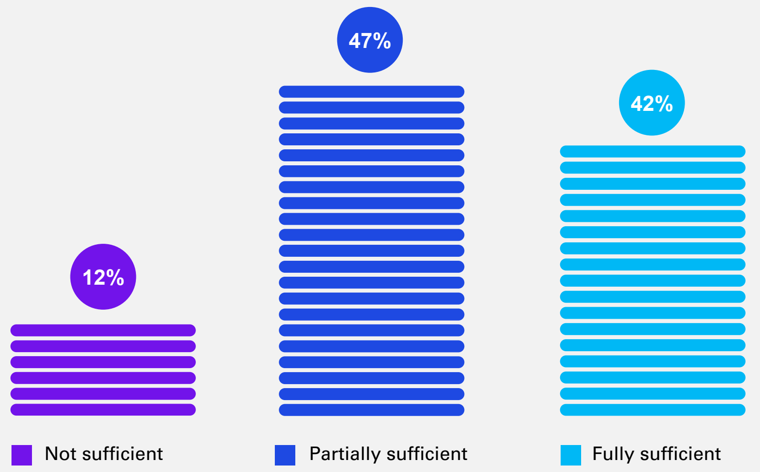
Frequency of risk assessment



In-life product review process



Budget for cross-functional corrective actions

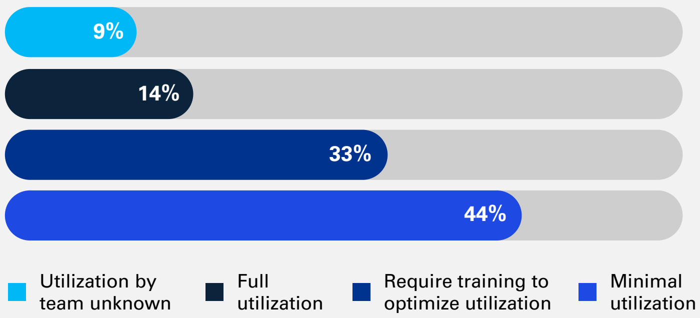


RAFM practices show partial strategic alignment. While some organisations have defined roadmaps and governance processes, many rely on reactive risk assessments and face budget constraints. Strengthening alignment, proactive monitoring, and funding is key to improving RAFM maturity.

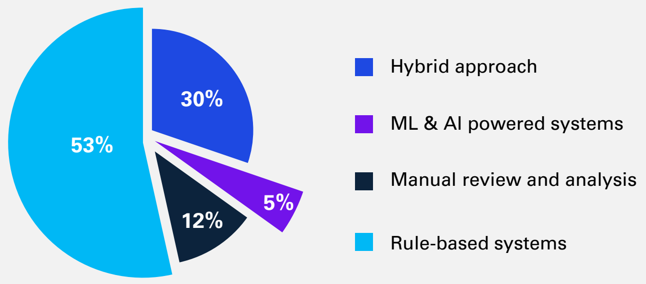
Technology, automation & AI/ML adoption

The survey highlights a significant shift in RAFM functions, with widespread adoption of advanced technologies such as Artificial Intelligence (AI), Machine Learning (ML), Robotic Process Automation (RPA), and Data Analytics. These tools are being leveraged to drive end-to-end automation, enhance fraud detection capabilities, and optimize revenue assurance processes across industries.

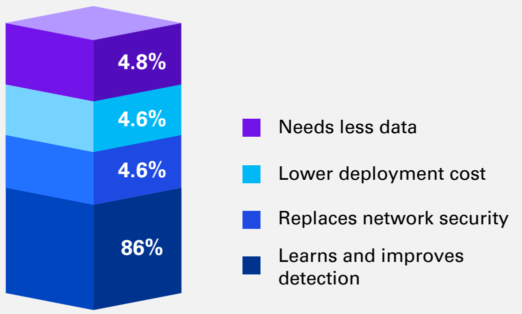
Tech (AI/ML/RPA) utilisation



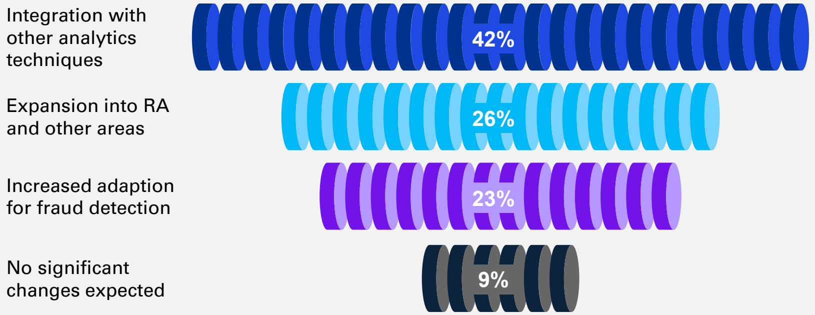
Fraud detection automation levels



AI/ML in SIMBOX detection



Projected evolution of AI/ML in RAFM



> "More than ever before, AI-enabled RAFM is significantly enhancing operational efficiency and reducing revenue leakage whilst expanding the function's coverage"

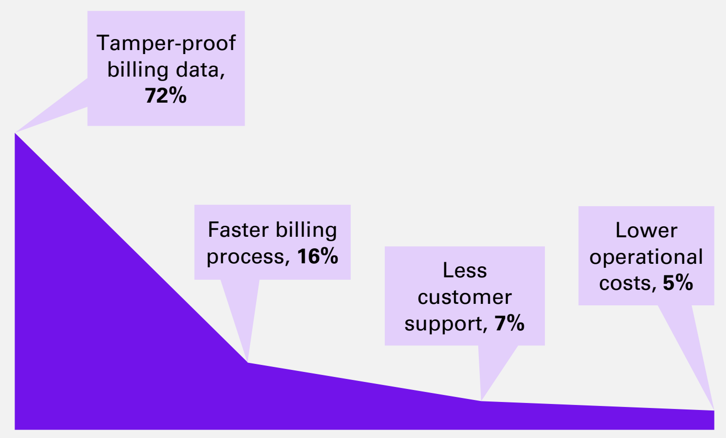
Thomas Gouws
Partner, COO Advisory
KPMG SA

> "In a fast-paced transformative world from RA to BA, the objective of RAFM operations would not be spend time on how to build insights with complex queries but what insights can one bring to business for informed decision making. AI can prove to be a power catalyst for the same, drastically improving TAT on operations and becoming outcome driven."

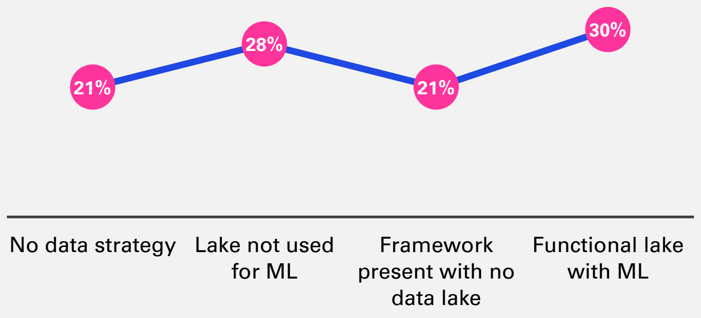
Rahul Hakeem
Partner, TMT,
Risk Advisory
KPMG in India

RAFM operations are increasingly leveraging AI/ML, RPA, and data analytics for automation, fraud detection, and optimization. Most teams use hybrid or manual approaches, with limited full tech adoption and training needs. Emerging technologies like blockchain and data lakes are enhancing security and enabling future-ready ML applications.

Blockchain impact on HLR billing



Data lake readiness for ML



RPA in fraud detection

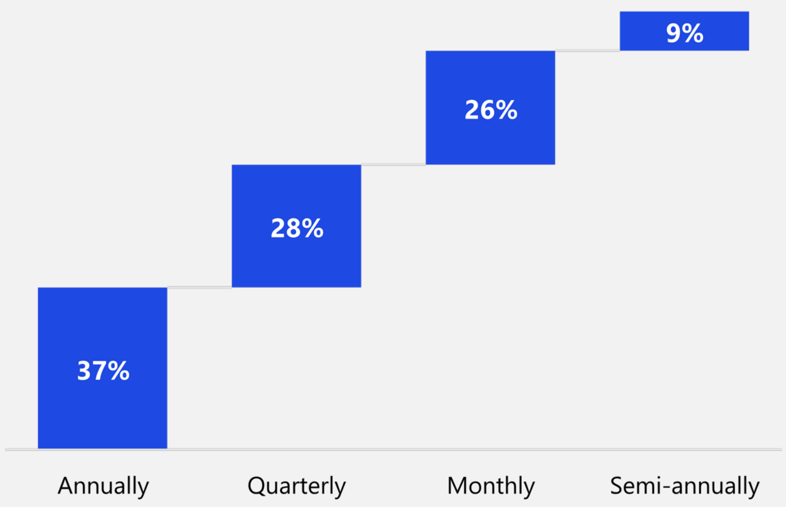
> A few years ago, Revenue Assurance & Subscriber Fraud were segmented into Operations and Monitoring and have over time played catch-up in a more reactionary mode of supporting the business. Fast forward to present day with RAFM embedding more Robotics and Dynamic Analytics in the assurance function, the responsibility on the RAFM function has escalated. Products and Services are a lot more complex today and APIs are proliferated in a lot more convoluted way, with Telcos plugging into Fintechs, VAS providers, Insurance, Switch Partners etc. Our RAFM Global Survey spotlights some of the recent challenges facing the modern day RAFM.

Lawrence Amadi
Head of Telecom, KPMG Nigeria

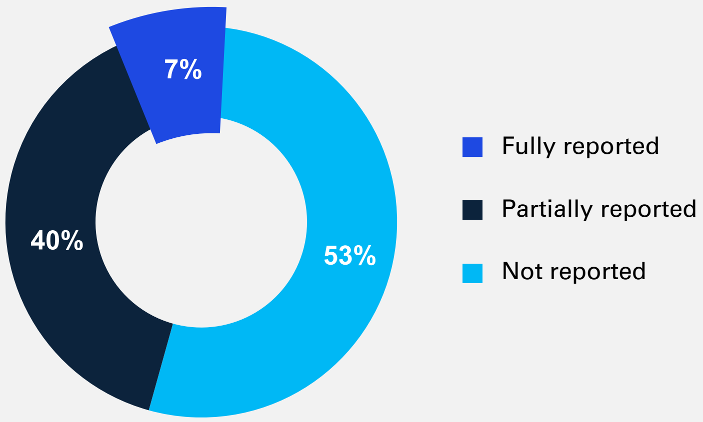
Control testing & effectiveness

This section presents findings from the survey on how frequently RA and FM controls are tested for accuracy and efficiency. It also highlights how effectively organizations identify and communicate control gaps and risks. The results underscore the importance of consistent validation practices and transparent risk reporting across entities.

Frequency of control testing



Control reporting breakdown status



> Future-fit RAFM harnesses AI, ML and RPA to shift from hindsight to foresight—automating the grind, amplifying insight and staying always ahead of risk

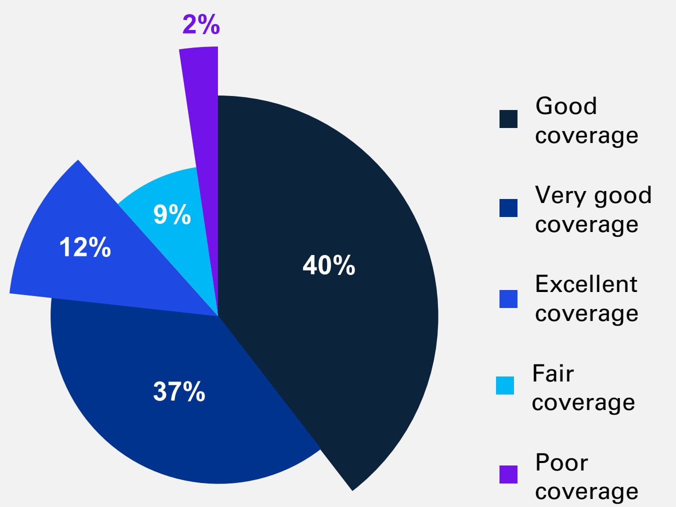
Yuvi Rajha
General Manager - RAFM
MTN Group

RA and FM controls are tested with varying frequency, most commonly annually, quarterly, and monthly to ensure logic accuracy and operational efficiency. While 53 per cent of controls are fully reported, 40 percent are only partially covered, indicating room for improvement in transparency. Leakage identification and reporting remain critical, with efforts focused on aligning control coverage with key risk areas and revenue streams.

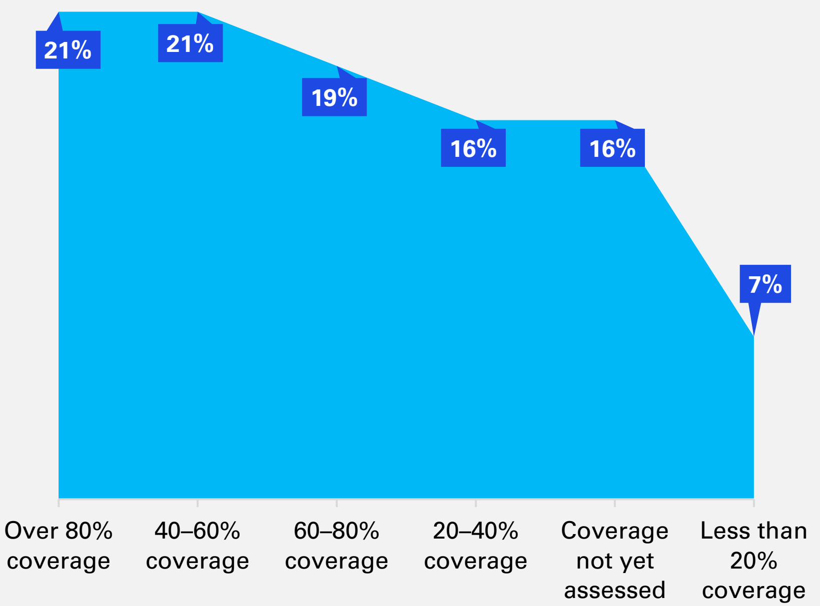
Reporting & risk coverage

The survey assesses how well RAFM controls mitigate risks across diverse revenue streams and regulatory domains, based on internal ratings and reporting practices. It underscores the need for comprehensive coverage to ensure effective risk management and compliance.

Risk coverage rating scale



Regulatory risk control coverage



> With the rapid advancements in the Telecom ecosystem and AI technologies, we are on the cusp of a transformative era for Revenue Assurance and Fraud Management. These innovations will enable organisations to deploy proactive controls that anticipate potential issues before they arise. By empowering companies to leverage historical data trends, process automation, and intelligent machine learning algorithms, they can significantly improve their risk mitigation strategies and optimize their operational efficiency. This shift will not only safeguard revenue but also create substantial value contributions that are essential for sustained growth and competitive advantage in today's dynamic market landscape.

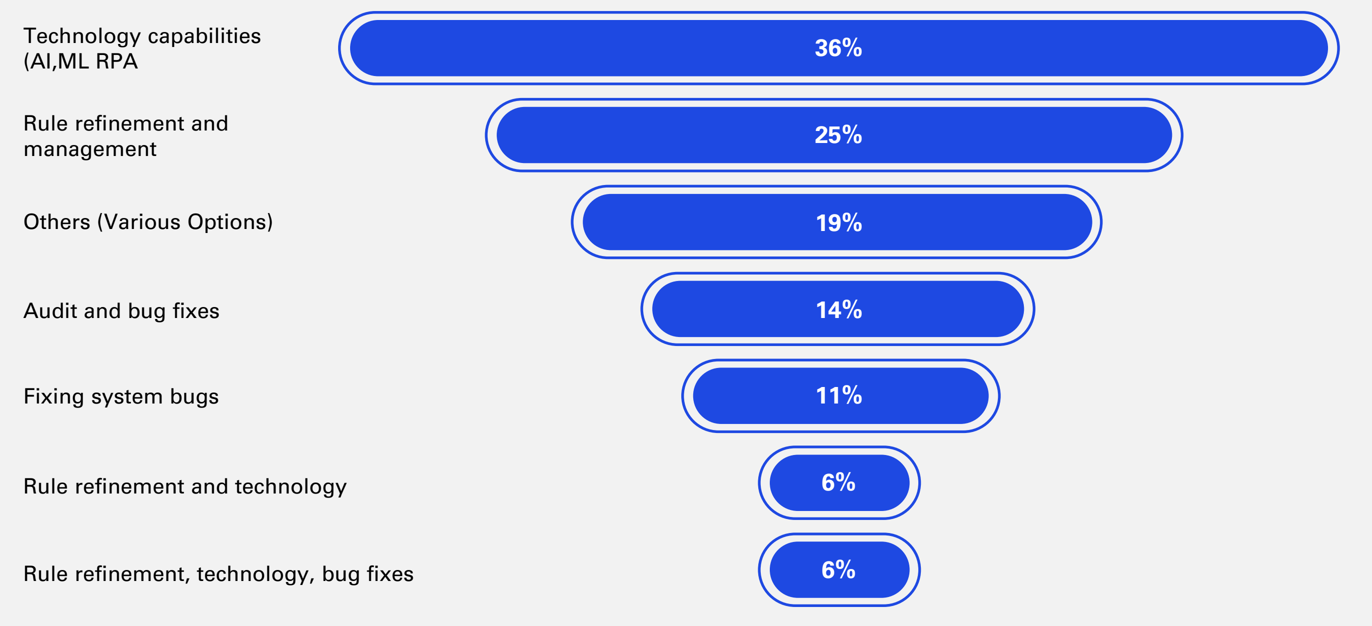
Amit Agarwal
Global Head – Revenue Assurance
Tata Communications

Most organisations rate their overall risk coverage as good to very good, though only 12 per cent report excellent coverage. Regulatory risk control coverage varies widely, with a significant portion yet to assess or falling below optimal thresholds, highlighting gaps in compliance readiness.

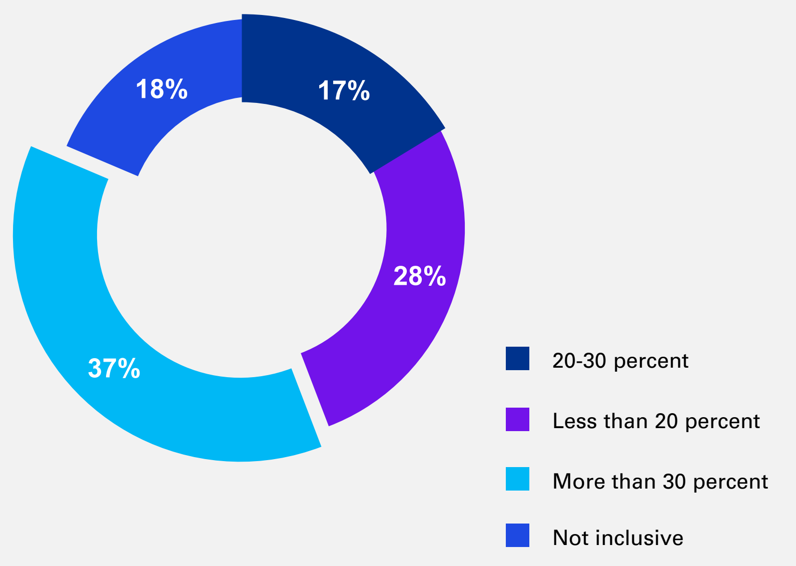
Change management & budget allocation

The survey findings highlights on how RAFM teams allocate their annual budgets, including provisions for RAFM control implementation, process improvements, and strategic initiatives. The results highlight the alignment between financial planning and operational resilience in addressing revenue assurance and fraud risks.

RAFM budget allocation activities



RAFM in business change management and enhancement budget

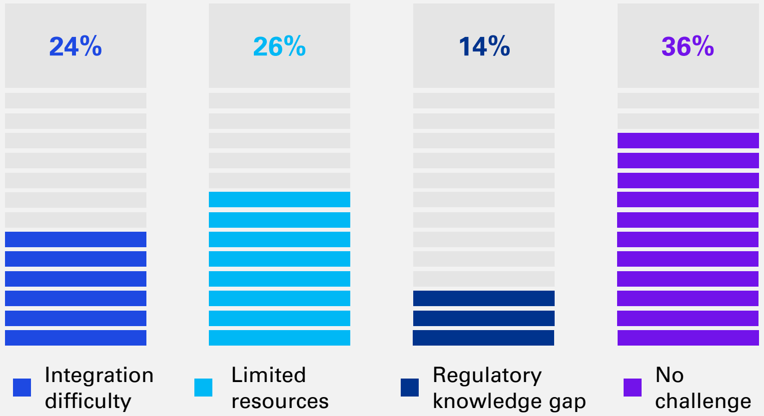


RAFM budgets are primarily directed toward control implementation, process improvements, and technology upgrades. Many organisations also include RAFM activities in broader business change and enhancement budgets, reflecting a strategic approach to integrating risk management with operational development. This alignment supports stronger financial planning and resilience in fraud and revenue assurance efforts.

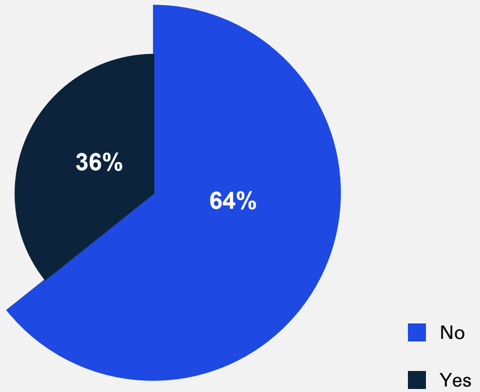
Regulatory compliance

Regulatory compliance in RAFM focuses on overcoming key challenges, ensuring budget support, and aligning goals with regulatory expectations. It also defines assurance scope for regulators to maintain transparency and control integrity.

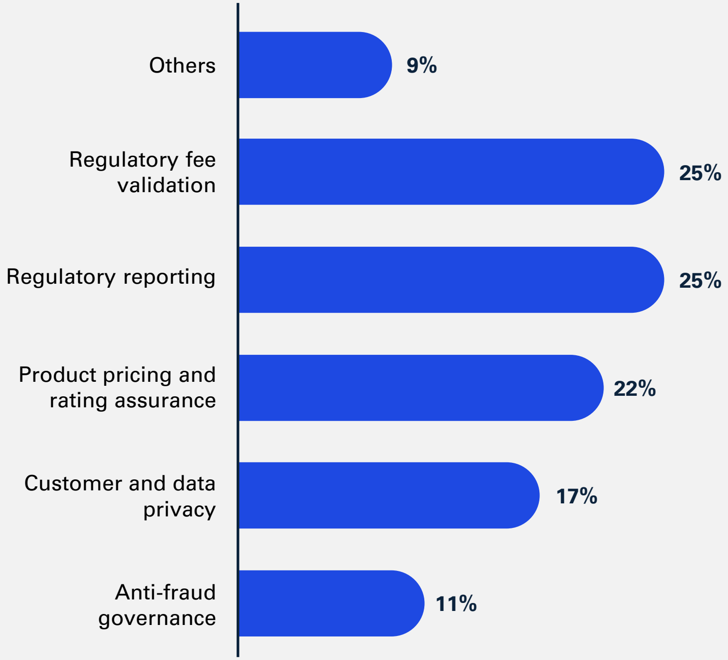
Primary compliance challenge



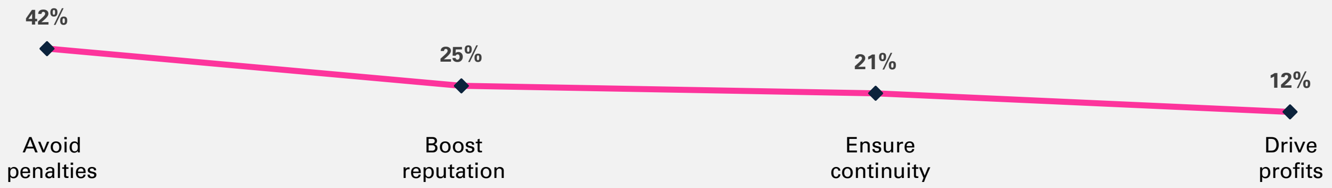
RAFM compliance monitoring budget



Key assurance areas covered in scope by regulatory bodies



Compliance goal map

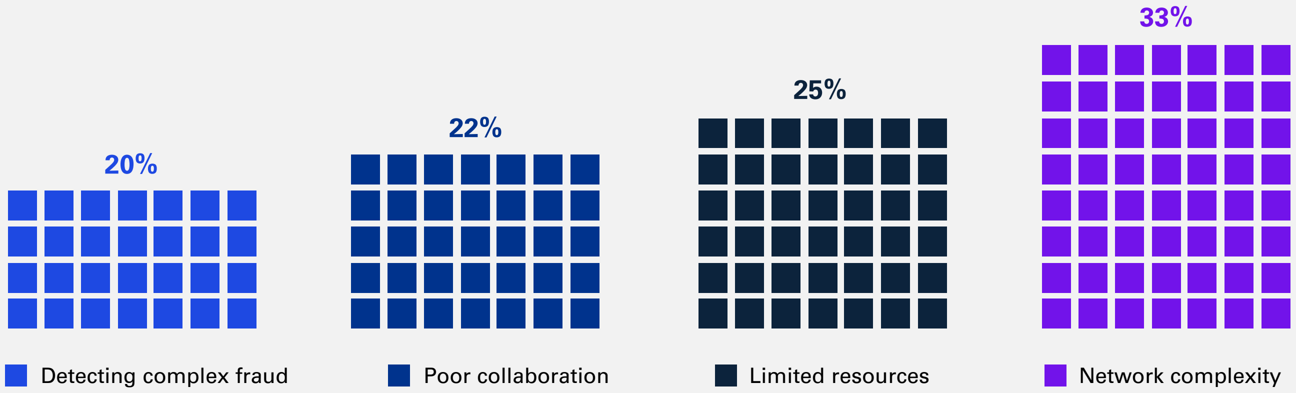


Limited resources and regulatory knowledge gaps are top compliance hurdles. RAFM assurance focuses on revenue, fees, and pricing, with most teams budgeting for monitoring. Avoiding penalties and boosting reputation are the main compliance goals.

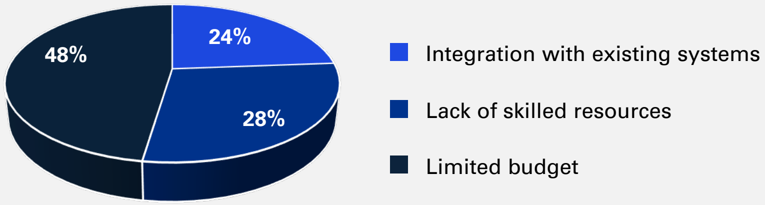
Challenges & opportunities

RAFM teams are navigating operational challenges and facing barriers to adopting advanced technologies and techniques. At the same time, they are identifying promising trends and opportunities that could reshape the RAFM landscape over the next few years, driving innovation and strategic growth.

Key challenges faced



Challenges in adopting advanced RAFM technologies



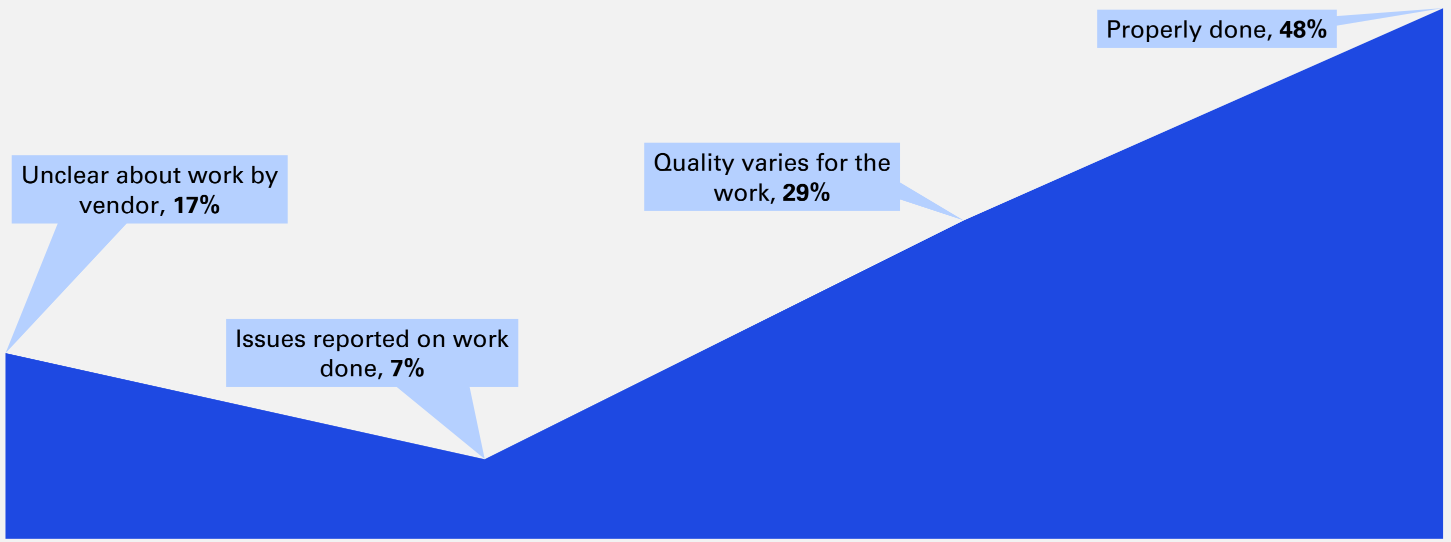
> Over the last decade, RAFM has evolved from traditional rule-based semi-automated controls and leakage detection to end-to-end automation, with greater emphasis on embedded analytics. We are in a midst of transition from static framework to more dynamic and data-driven intelligence that focusses on foreseeing risks instead of merely reacting to them. With the advent of AI and real-time insights, the focus will further shift toward smarter, more proactive strategies to protect and enhance revenue.

Yash Mohan
Head of RA,
Emtel, Republic of Mauritius

Vendor & deployment quality

Vendor-led RAFM technology deployments require thorough documentation, rigorous testing, and structured handovers to ensure operational continuity and system reliability. This section examines how consistently these practices are followed, reflecting the quality and accountability of vendor engagement in deployment processes.

Vendor compliance in RAFM deployment



Nearly half of RAFM deployments are properly executed, but 29 per cent show inconsistent quality and 17 per cent lack clarity. This highlights the need for stronger vendor oversight and standardized deployment practices. Regular audits and feedback mechanisms can help improve consistency and reliability.

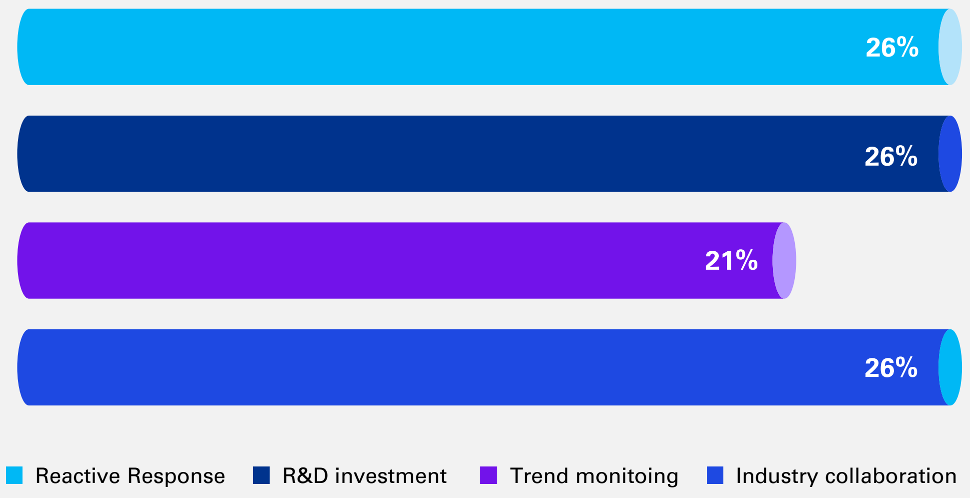
> In an era where digital transformation accelerates telecom innovation, robust Revenue Assurance and Fraud Management is no longer just a safeguard, it's a strategic enabler. As margins tighten and fraud tactics evolve, RAFM must transform into a proactive, intelligence-driven function that ensures every byte of data and every cent of revenue is accurately captured. By anticipating risks and embedding resilience, RAFM plays a critical role in protecting profitability, sustaining trust, and enabling sustainable growth in a hyper-connected world.

Shukrullah Hamdard
Sr. Manager, RAFM, ATOM Afghanistan

Fraud threat preparedness

Organisations are increasingly adopting proactive strategies to counter emerging fraud threats and revenue assurance challenges. This part of the survey explores how teams stay ahead through early detection, strategic planning, and technology-driven approaches to fraud prevention.

Approach to emerging RAFM fraud threats



Organisations are taking a balanced approach to emerging fraud threats in RAFM, with equal emphasis on reactive responses, R&D investment, trend monitoring, and industry collaboration. This indicates a strategic blend of short-term mitigation and long-term innovation. Equal prioritization suggests that no single method dominates, highlighting the need for integrated fraud preparedness. Such diversification strengthens resilience against evolving risks.

> We're witnessing a clear shift in RAFM toward proactive, analytics-driven frameworks that leverage AI and automation to detect leakages and fraud in near real-time. The focus is rapidly moving from traditional controls to predictive insights, with a strong emphasis on safeguarding customers and shareholder's trust. Moreover, RAFM is rapidly evolving from "Traditional RAFM" to "Business Assurance" with the emphasis on real-time risk mitigation.

Anonymous

Head - Revenue Assurance & Fraud Management, Leading Telecom Operator in Middle East

> In the AI era, the focus of Revenue Assurance (RA) and Fraud Management (FM) has evolved significantly, driven by the complexity and volume of data, digital transformation, and the rise of intelligent automation. We should focus on Proactive and Near Real time Leakage detection and real-time Fraud prevention. The coming RAFM system has to be AI enabled and using Robot to minimize human effort and maximize the prevention.

Anonymous

Head - Revenue Assurance & Fraud Management, Leading Telecom Operator in South East Asia

Chapter 1

How technology has influenced and transformed revenue assurance

- Static, rule-based checks and post-event reconciliations are being replaced by intelligent systems using real-time analytics, automation, and predictive intelligence
- Advanced AI tools study historical data and user behavior to identify complex fraud patterns and predict fraudulent activities in advance
- Analytics are used to assign real-time risk scores to partners, customers, and processes
- Digital assistants and AI generators produce fraud alerts, dashboards, and anomaly summaries with minimal human involvement
- Automated tools extract information from unstructured documents like contracts and TAP/RAP files, speeding up reconciliation and compliance
- AI-powered translators and code generators help interpret legal language and quickly produce SQL queries or Python scripts for analysis
- Many organisations use AI and RPA tools in isolation without full integration into overall assurance workflows, to increase their effectiveness these tools needs to be integrated in the overall execution framework
- Industry consensus is that RAFM will become tightly linked to technology, with a need to scale solutions beyond pilot projects

> "As artificial intelligence advances rapidly, the field of revenue assurance and fraud management must evolve in parallel—deploying systems that continually adapt, deliver real-time insight, enforce zero trust policies, and proactively detect emerging threats."

Anonymous

Associate Director - Revenue Assurance & Fraud Management
Leading Telecom Operator Group in Middle East

Chapter 2

Key focus areas of transformation from RA to BA

The survey also confirms a fundamental shift in mindset from Revenue Assurance as a back-office control function to Business Assurance as a proactive, value-protecting enterprise layer. This evolution is rooted in the realization that assurance is no longer confined to leakages or billing mismatches but extends to customer experience, partner accountability, operational governance, and margin preservation. Many organisations are now aligning assurance KPIs with strategic business objectives, making it essential for RAFM units to collaborate with product, commercial, and partner teams. This shift is also reflected in the growing attention on new assurance areas such as service activation integrity, product lifecycle validation, and revenue recovery across partner ecosystems.

- Real-time value assurance is emerging, requiring assurance decisions to be made instantly, often during service delivery or at the start of a transaction
- This shift is driving demand for real-time data ingestion, contextual analytics, and scalable governance frameworks
- The RAFM team's role is evolving from merely conducting post-event checks to acting as a strategic partner
- The team is now responsible for protecting enterprise value, improving operational efficiency, and supporting digital transformation goals

> In the age of Agentic AI, assurance transcends detection—it becomes anticipation. Business Assurance evolves into a strategic nerve center, where AI accelerates insight, automates precision, and fortifies resilience at scale.

Arjun Malhotra
Partner, TMT
KPMG in India

Chapter 3

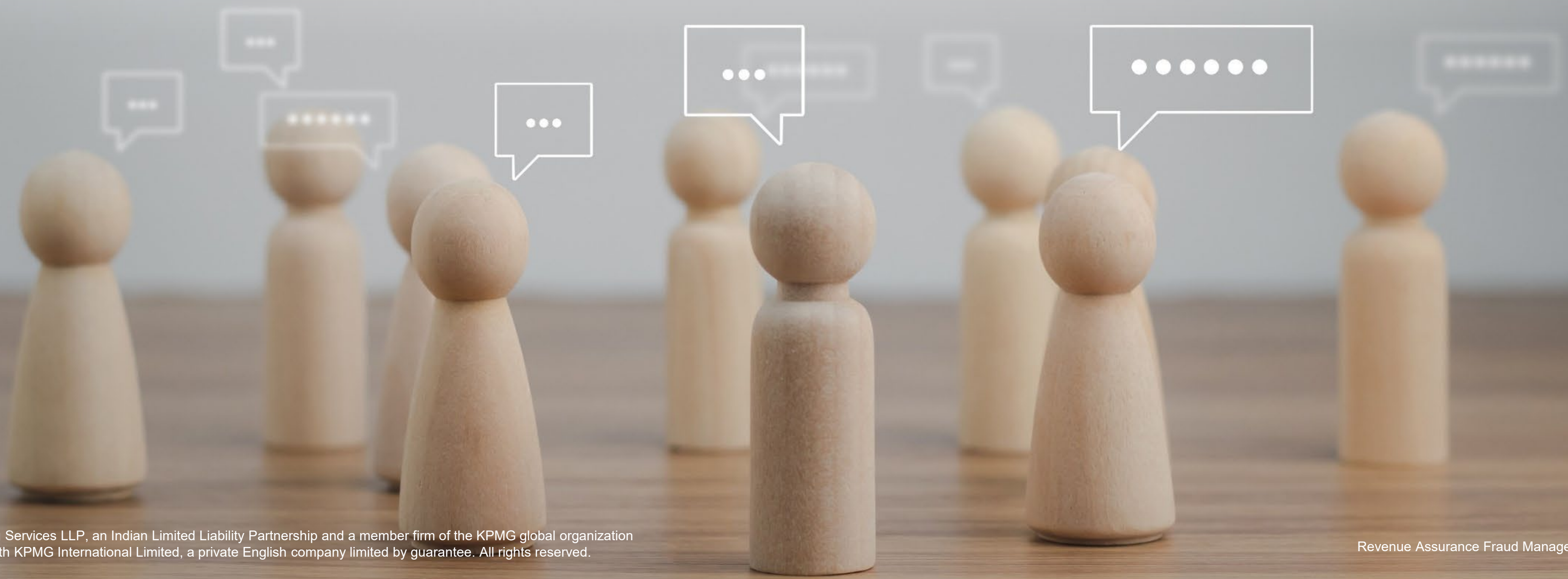
Leveraging the business assurance framework across and beyond telecom

- The survey reveals that the Business Assurance (BA) framework is increasingly applicable beyond the telecom sector
- Within telecom, BA is expanding to areas such as data centers (for usage tracking), fintech (for transaction integrity and fraud analytics), and partner management (for automated revenue sharing margin assurance and B2B contract compliance and SLA assurance)
- BA serves as a unifying layer that integrates processes, risk management, and value alignment across complex digital ecosystems
- Outside telecom, BA models are being adapted across industries including healthcare, hospitality, aviation, logistics, and utilities
  - **Healthcare sector:** Business assurance frameworks are used to verify insurance claims, monitor patient adherence to prescribed treatments, and promote effective collaboration between insurers and healthcare providers.
  - **Aviation Sector:** Companies utilize BA framework to monitor operational expenses across different departments, assess the profitability of various flight routes, and streamline maintenance planning.
  - **Hospitality Sector:** Business assurance framework helps to maintain accurate dynamic pricing and minimize the risk of inventory loss.
  - **Logistics Sector:** Companies implement BA framework to manage the shipment-to-payment lifecycle and uphold regulatory and contractual compliance among third-party service providers.
  - **Utilities Sector:** BA frameworks are implemented in their meter-to-cash workflows to detect potential billing inaccuracies, uncover fraudulent activities, and prevent improper allocation of subsidies.

- These diverse use cases highlight BA's scalability and flexibility, enabling organizations to focus on value flows, reduce operational risks, uncover gaps, and strengthen both customer-facing and backend operations.

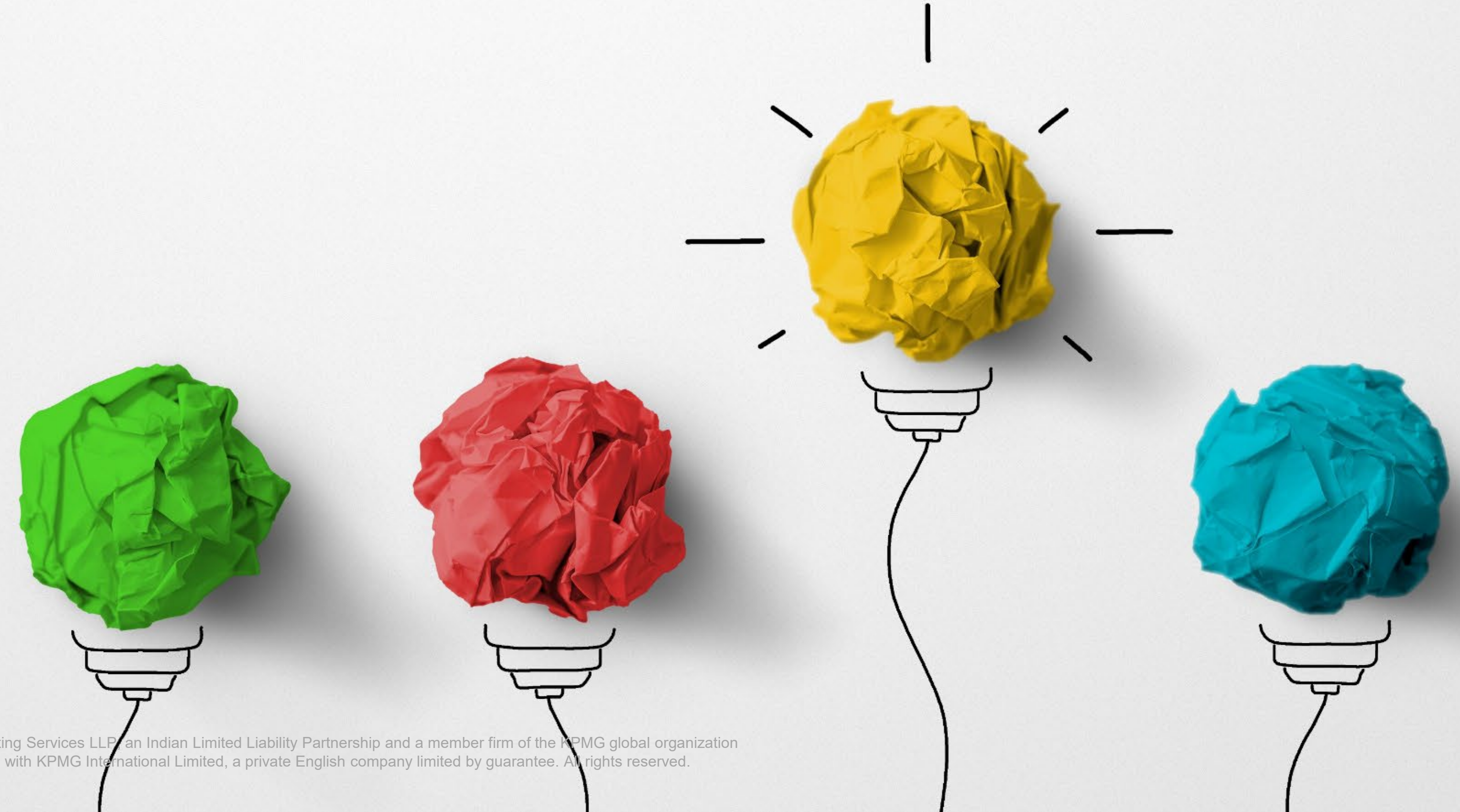
Survey methodology

To ensure broad relevance, the survey included inputs from a diverse mix of organisations, with a focus on telecom players across regions and service models. Data was collected through a structured online digital survey. The approach was both quantitative and qualitative capturing numerical insight (such as automation coverage, or AI adoption) and contextual narratives around organisational intent, capability bottlenecks, and roadblocks to transformation. The survey design revolved around five core pillars: strategic alignment, operational execution, technology infusion, fraud risk posture, and readiness to adopt business assurance frameworks. The objective was not just to benchmark maturity levels but to understand the practical enablers and inhibitors shaping this journey from traditional RAFM to a more integrated, tech-driven, and business-aligned assurance model.



Conclusion

The 2025 RAFM Survey paints a picture of an industry in the middle of transformation- facing clear challenges in automation, integration, and skill development, but also showing strong intent and vision for the future. Revenue Assurance is no longer a niche compliance activity. It is evolving into Business Assurance: a central nervous system that safeguards revenue, optimizes operations, and fuels data-driven decision-making. The survey results make it clear that success in this transformation journey depends on how effectively organisations integrate technology, expand their assurance scope, and build collaborative frameworks that align with broader business goals. Those who can do so will be well-positioned to navigate complexity, unlock value, and lead confidently in the digital era.



Glossary

RAFM	Revenue Assurance and Fraud Management
AI/ML	Artificial Intelligence / Machine Learning
RPA	Robotic Process Automation
VAS	Value-Added Services
Fintech	Financial Technology
BA Framework	Business Assurance Framework
SLA	Service Level Agreement
HLR	Home Location Register
TAP	Transferred Account Procedure
RAP	Returned Account Procedure
SQL	Structured Query Language

Acknowledgements

Authors

Purushothaman KG
Partner, TMT
Head - Technology Transformation & Telecommunication
KPMG in India

Rahul Hakeem
Partner, TMT
Risk Advisory
KPMG in India

Arjun Malhotra
Partner, TMT
Risk Advisory
KPMG in India

Contributors

Avinash CH
Associate Director
Risk Advisory
KPMG in India

Arnab Mohapatra
Manager
Risk Advisory
KPMG in India

Mridula Sinha
Assistant Manager
Risk Advisory
KPMG in India

Pousha Prabhu
Consultant
Risk Advisory
KPMG in India

Payal Kumari
Associate Consultant
Risk Advisory
KPMG in India

KPMG in India contacts:

Akhilesh Tuteja
Head – Clients & Markets
National Leader – Technology
Media and Telecom
E: atuteja@kpmg.com

Purushothaman KG
Partner- Advisory
Head - Technology
Transformation &
Telecommunication
E: purushothaman@Kpmg.Com

Rahul Hakeem
Partner, TMT
Risk Advisory
E: rahulhakeem@kpmg.com

Arjun Malhotra
Partner, TMT
Risk Advisory
E: arjunmalhotra1@kpmg.com

kpmg.com/in

Access our latest insights on KPMG Insights Edge

Follow us on:
kpmg.com/in/socialmedia

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.