The Case of Alpha Consulting:

Preparing Auditors for a Compliance-Driven Future

Jayant Palan - Co-founder & Program Director-GRMI
Harshal Mokashi, Yogita Dua, Prajakta Buggewar, Shreyansh – Scholars
Global Risk Management Institute

Synopsis

This case study examines how Alpha Consulting, a global professional services firm specializing in compliance, cyber risk, and regulatory assurance, redesigned its assurance function to maintain compliance readiness in an increasingly complex global regulatory environment. Through Project Compliance 360, the firm transformed its audit methodology, strengthened regulatory intelligence capabilities, and enhanced auditor skillsets to position itself as a trusted governance, risk, and compliance (GRC) partner. The case explores the challenges faced, actions taken, outcomes achieved, and implications for internal auditors operating in similar environments.

Context / Background

The last decade has witnessed an exponential rise in compliance obligations across industries. Regulators around the world have introduced or updated frameworks such as the EU GDPR, California's CCPA, India's DPDPA 2023, EU AI Act (2024), ISO 37001 Anti-Bribery standards, and NIST Cybersecurity Framework 2.0 (2024), significantly escalating the demands placed on organisations.

Alpha Consulting, headquartered in London with operations in 32 countries, provides internal audit, risk advisory, cybersecurity, and compliance readiness services. While historically strong in governance, the firm's audit approach was less mature in areas requiring:

- Cybersecurity integration
- Emerging technology controls
- Real-time regulatory intelligence
- Cross jurisdictional compliance capability

By 2024–25, client expectations shifted dramatically. Boards increasingly demanded:

- Proactive compliance assurance
- Real-time risk visibility
- Integrated cyber-compliance audits

- Auditors capable of interpreting global regulatory requirements

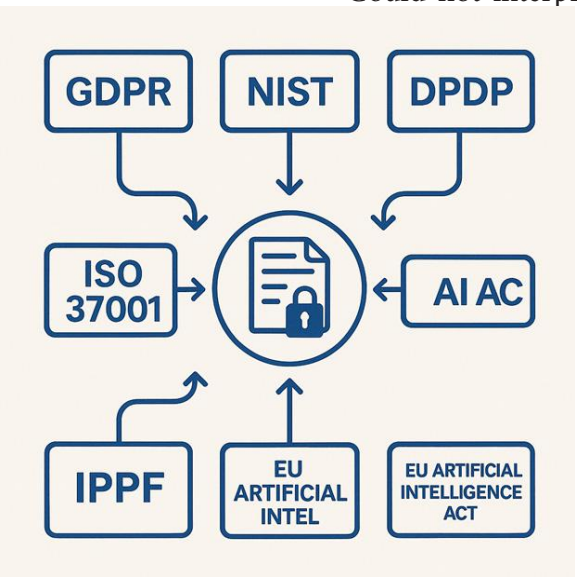
High-profile client incidents, including privacy penalties, third-party bribery risks, and cyber supply-chain failures, highlighted Alpha's capability gaps. Recognizing the urgency, Alpha launched Project Compliance 360.

Case Narrative

Alpha's internal audit function confronted three significant capability gaps:

1. Disconnect in Regulatory Intelligence

Auditor teams lacked timely and consistent understanding of rapidly evolving compliance requirements. Examples included:



- Asia-based privacy auditors misinterpreting GDPR developments emerging from Europe
- Cyber auditors not fully understanding updates in NIST CSF 2.0 or emerging AI governance regimes.

This led to audit inefficiencies, inconsistent interpretations, and potential compliance misalignment.

2. Siloed Cyber and Compliance Audits

Audits were executed independently, resulting in duplicated testing and incomplete risk visibility. Clients increasingly sought integrated assurance covering:

- Data privacy
- Cybersecurity
- Third party governance
- Anti-bribery compliance
- Digital controls
- Operational resilience

The absence of a unified methodology created blind spots and fragmented reporting.

3. Inadequate Skills for Technology driven and automated compliance:

Regulators, especially in financial services, employed AI enabled surveillance and automated monitoring. Many auditors at Alpha:

- Lacked familiarity with RegTech enabled compliance analytics
- Were unable to audit automated systems and digital control environments
- Could not interpret or comprehend machine-generated compliance dashboards

Clients demanded auditors capable of testing automated controls, evaluating cyber resilience, and analyzing real-time compliance signals.

Transformation under Project Compliance 360

Alpha's leadership implemented a three pillar transformation program.

A. Regulatory Intelligence Hub

Alpha developed a centralized unit to keep track of compliance updates from:

- National and regional regulators
- Cybersecurity authorities
- Anti-Bribery enforcement authorities
- Industry and sector specific watchdogs

The hub published a "Compliance Readiness Bulletin" every week summarizing regulatory changes, interpretation of new requirements mapped directly to audit procedures and integration of regulatory updates in the firm's Governance, Risk, and Compliance (GRC) platform.

This initiative significantly improved consistency and reduced regulatory misinterpretation across regions.

B. Integrated Compliance Audit Methodology

Alpha redesigned its methodology to combine compliance, cybersecurity, and technology assurance through:

- Cross mapping controls of ISO 27001, NIST CSF, SOC 2, GDPR and Anti-bribery frameworks

- Introduction of cyber-compliance walkthroughs
- Inclusion of threat intelligence within compliance testing
- Expanded testing of digital controls, such as MFA, encryption, and data loss prevention
- Unified reporting structures providing holistic risk narrative

This integrated approach aligned Alpha's audit function with contemporary global risk expectations.

C. Skills Enhancement and Certification Approach

A mandatory capability roadmap was established for all audit professionals, including:

- CIA and CRMA (Internal Audit & Risk)
- CISA or CEH (Cyber assurance)
- GDPR DPO certification
- ISO 37001 Lead Implementer (Anti-Bribery)
- AI compliance and model governance modules
- These initiatives measurable strengthened audit quality, credibility and client trust.

Impact of Project Compliance 360

Within 12 months, Alpha achieved significant outcomes:

- Findings of regulatory non-compliance decreased, by 40 percent, across audit engagements
- Improved customer satisfaction by 27%
- Repeat business for cyber-compliance services increased by 33%
- Audit cycles decreased by 20% from method integration.

Alpha successfully repositioned itself from a traditional audit advisory provider to a future ready compliance assurance partner.

Discussion Questions

- What were the primary gaps in Alpha Consulting's compliance readiness and how did these affect audit quality?
- How did the creation of the Regulatory Intelligence Hub provide insight to reinforce Alpha's audit methodology?
- In what ways would the inclusion of cybersecurity increase the audit's ability to identify risk?
- Which skills should internal auditors focus on developing, to ensure their future readiness in an increasingly regulated global environment?
- If you were responsible for an internal audit function, what else would you do to enhance the internal compliance maturity level?

Conclusion

The Alpha Consulting case highlights that compliance readiness is no longer optional, it is central to the internal audit value proposition. Global regulatory shifts in data privacy, cyber security, ESG, anti-bribery and AI governance, require internal auditors to evolve continuously.

Project Compliance 360° demonstrates that audit function must build:

- Consolidated intelligence of regulation and compliance requirements
- Enhanced and multidisciplinary auditor skillsets
- Integrated cyber-compliance methodologies
- Proactive, technology assisted compliance testing
- Audit functions that embrace these capabilities will become strategic partners to management, providing assurance in an environment defined by interconnected risks and rapidly evolving regulations.

Learning Objectives

After studying this case, learners should be able to:

- Explain the importance of compliance readiness within internal audit functions.
- Assess how global regulatory developments influence audit methodologies.
- Analyze the role of cyber security integration in modern compliance audits.
- Identify key auditor competencies for multi-jurisdictional regulatory environments.
- Evaluate ways for enhancing audit methodologies through technological upgrade and intelligence systems.

Modern Auditing in Indian FinTech:

Ensuring Compliance through AML and KYC Audits

Ruchika Rai - Compliance Officer, Phillips India & Visiting Faculty -GRMI
Vanya Singh, Harshdeep Gangawane, Saurabh Kashyap & Shivani Rajwar – Scholar
Global Risk Management Institute

Abstract

India's FinTech sector has transformed the financial services landscape, particularly in digital payments and wallet-based systems. However, this rapid growth has heightened exposure to money laundering, fraud, and customer due diligence failures. This case study examines key enforcement actions by the Reserve Bank of India (RBI) against Paytm Payments Bank Ltd. (PPBL) for persistent Anti-Money Laundering (AML) and Know Your Customer (KYC) lapses and highlights the implications for internal auditors, compliance officers and risk practitioners. The study underscores the necessity for robust internal control, periodic AML/KYC audits, governance structures, and technology-enabled monitoring within FinTech entities.

Industry Context / Background

India's FinTech industry has gone through a drastic change in the past ten years and has become an essential factor in digital finance. Digital adoption, UPI led payments growth, smartphone penetration, and regulatory support have made India one of the fastest growing digital payment markets globally. In October 2024 alone, UPI processed 16.58 billion transactions worth Rs 23.49 lakh crore, reflecting the scale and velocity of digital payment activities.

This upward trend is backed by the growing number of mobile phone users, the government-supported initiatives such as Demonization and Digital India, and the favourable regulatory framework. While this growth has enabled financial inclusion, it has also intensified inherent risks, particularly in AML/CFT, identity fraud, mule accounts, synthetic identities, and high-velocity transactions.

India's AML/KYC regime is governed by:

- The Prevention of Money Laundering Act (PMLA), 2002
- RBI's Master Direction on KYC (2016, updated 2025)
- FIU-IND reporting requirements
- KYC obligations for Payment Aggregators (2020 guidelines)

These frameworks require financial institutions and FinTech companies to perform customer due diligence, verify beneficial ownership, monitor transactions, and report suspicious activity. Despite this, compliance maturity varies significantly across FinTechs, especially those with limited in-house compliance and internal audit capacities.
RBI enforcement actions, particularly between 2021–2023, surged nearly 88%, with AML/KYC violations constituting the majority of penalties. India's 2024 FATF Mutual Evaluation review rated India largely compliant, but effectiveness gaps remain, especially in supervision of non-banking and FinTech entities.

Case Study: Paytm Payments Bank – A Compliance Audit Failure

The enforcement action against PPBL is one of the most significant AML/KYC compliance failures in India's FinTech landscape. The RBI, in the early part of 2024, ordered PPBL to stop deposits and credits from 29th February, 2024, which resulted in freezing of customer accounts.

Key Failures Identified

A third-party audit commissioned by the RBI in 2022 uncovered critical lapses:

- Existence of hundreds of thousands of non-KYC or partially-KYC accounts
- Multiple accounts using a single PAN, violating regulatory norms
- Wallet and transaction limits exceeding permissible thresholds for minimum-KYC accounts
- Incomplete or fictitious customer profiles
- Insufficient monitoring of high-value or high-velocity transactions
- Weak internal controls and inadequate system alerts

RBI responded by:

- Restricting the onboarding of new customers (2022)
- Mandating a comprehensive system audit and rectification plan
- Citing the bank as "non-compliant with regulatory standards" (2024)
- Directing cessation of deposits and credit transactions (2024)
- Ordering closure of nodal accounts due to operational irregularities

Subsequently, the Enforcement Directorate (ED) initiated investigations under PMLA, uncovering misuse of wallets for illicit lending-related flows.

Internal Audit Implications

The PPBL case emphasizes the consequences of audit gaps:

- Internal audit did not detect or escalate large scape KYC anomalies
- Governance mechanisms failed to ensure timely remediation
- Technology systems were not adequately tested or validated by audit teams
- Risk assessments did not recognize AML/CFT as a top-tier risk
- Audit independence and reporting lines required strengthening

This failure demonstrates the need for integrated assurance, where internal audit, compliance, risk, and technology functions operate cohesively.

Discussion Questions for Internal Audit Professionals

Regulatory Failures:

- What specific AML/KYC breaches were identified at PPL?
- How did these failures elevate systemic risk for customers, partners, and the broader payment ecosystem?

Audit Oversight:

- Could internal audit or second line compliance functions have identified these gaps earlier?
- How should internal audit approach system audits, customer lifecycle reviews, and control testing in FinTech environments?

Balancing Innovation vs. Compliance: FinTech business models prioritize scale and speed.

- What governance frameworks help balance innovation with AML/KYC compliance?
- How should internal audit evaluate new product launches, onboarding processes, and algorithm-based decisioning?

Preventive Measures for FinTec Startups: Recommend practical steps across Technology, People, Processes and Audit:

- AI-enabled transaction monitoring, anomaly detection, e-KYC validation tools
- Skilled AML analysts, audit specialists, data governance teams
- Risk-based KYC, enhanced due diligence for high-risk users, continuous monitoring, independent validation
- Regular AML/KYC audits, model validation, data quality audits, governance reviews

Conclusion

The PPBL enforcement action highlights an essential truth: FinTech innovation cannot come at the cost of regulatory compliance. For sustainable growth, digital financial institutions must embed AML/KYC controls into the technology stack, governance model, and product lifecycle.

Internal audit plays a pivotal role by:

- Conducting independent assurance on customer due diligence processes
- Validating transaction monitoring systems
- Identifying systemic control gaps
- Ensuring timely corrective actions
- Advising on emerging risks and regulatory expectations

As India's digital payments ecosystem continues to expand, internal auditors must evolve, deepen domain expertise, and leverage data-driven audit methodologies. Compliance should be treated not as a constraint, but as a cornerstone of risk resilience and long-term trust.

Learning Objectives

- Understand India's AML/KYC Framework: Get acquainted with the major components of India's AML/CFT laws (PMLA and rules) and the RBI's KYC/KYB standards, as well as their implications for FinTech industry.
- Analyse Compliance Risks: Identify patterns of fraud, mule accounts, and anomalies within FinTech customer and transaction ecosystem.
- Appreciate the Role of Internal Audit: Recognize how internal audit contributes to detecting control failures and triggering timely remediation.
- Apply Risk Management Practices: Develop and integrated compliance and audit approach leveraging technology, governance and process discipline.