Grant Thornton | 90 in Bharat and beyond

FACE

Fintech Barometer

Understanding the perception of risks amongst fintechs in India

July 2026

Table of Contents

Abbreviations

S. No.	Acronym	Full form
1	AA	Account Aggregator
2	AI	Artificial Intelligence
3	AML	Anti-Money Laundering
4	API	Application Programming Interface
5	BFSI	Banking, Financial Services and Insurance
6	CFT	Combating the Financing of Terrorism
7	CKYCR	Central KYC Records Registry
8	CRM	Customer Relationship Management
9	DLA	Digital Lending Application
10	DPI	Digital Public Infrastructure
11	DPDP	Digital Personal Data Protection (Act, Bill, or Rules)
12	DPIP	Digital Payments Intelligence Platform
13	e-KYC	Electronic Know Your Customer
14	GDP	Gross Domestic Product
15	IFSCA	International Financial Services Centres Authority
16	IoRS	Interoperable Regulatory Sandbox
17	IRDAI	Insurance Regulatory and Development Authority of India
18	KYC	Know Your Customer
19	LOS	Loan Origination System
20	LSP	Lending Service Provider
21	MDR	Merchant Discount Rate
22	ML	Machine Learning
23	MSE	Micro and Small Enterprise
24	NBFC	Non-Banking Financial Company
25	OCEN	Open Credit Enablement Network
26	PA	Payment Aggregator
27	PFRDA	Pension Fund Regulatory and Development Authority
28	PIDF	Payments Infrastructure Development Fund
29	RBI	Reserve Bank of India

Abbreviations

S. No.	Acronym	Full form
30	RBIH	Reserve Bank Innovation Hub
31	RE	Regulated Entity
32	SDF	Significant Data Fiduciary
33	SEBI	Securities and Exchange Board of India
34	SRO-FT	Self-Regulatory Organisation for FinTechs
35	TPAP	Third-Party Application Provider
36	TRAI	Telecom Regulatory Authority of India
37	UCC	Unsolicited Commercial Communication
38	ULI	Unified Lending Interface
39	UPI	Unified Payments Interface
40	YoY	Year-on-Year

Vivek Iyer

Partner and Financial Services Risk Consulting Leader

"India's fintech ecosystem has reached an important inflection point where long-term success will be defined not only by innovation and profitability, but by trust. As fintechs become increasingly embedded within the country's financial architecture, robust governance, responsible use of data, operational resilience, and customer centricity must evolve alongside growth. This report reflects the industry's collective perspective on the risks that matter most today and serves as a valuable guide for building a stronger, more resilient, and future-ready financial ecosystem."

Sugandh Saxena

CEO, FACE

"India's FinTech sector is gradually becoming integral to the financial ecosystem. Sustaining and deepening fintechs in the financial ecosystem and economy requires fintechs earning trust by creating value and firmly addressing risks as they emerge.

This report is an industry speak on FinTech's own perception and ranking of risks. A clear and common understanding of risks is the first step to prepare for and mitigate risks and drive individual and collective actions. We hope that report will contribute in that direction."

Context

India's fintech industry is now a mainstream, well-integrated part of the country's financial ecosystem. Unified payment interface (UPI), processing more than **20 billion digital payment transactions monthly**, has emerged as the world's largest real-time payments system. Other segments, such as digital lending, collectiontech, open finance, wealthtech, insurtech, and regtech, are scaling rapidly atop payment rails and digital public infrastructure (DPIs), such as Aadhaar, e-KYC, and Account Aggregator (AA). Fintechs are powering the aspirations and needs of emerging India for digital financial services that are convenient, suitable, affordable and secure.

Fintechs in India now transcend mere access with developments in open finance, alternative data and AI-driven underwriting, risk monitoring, servicing, and interfaces are changing how individuals and small businesses use financial services. Importantly, the fintech segment is thriving through collaboration with banks, NBFCs, and adjacent digital and real-economy sectors to unlock the potential of digital financial services for inclusive economic growth.

With this scale and success come novel risks; the threats of fraud and cybersecurity, compliance and ethics, continue to be concerns for the sector. Eventually, customer trust is the ultimate differentiator, and fintechs need to balance risks and innovation to earn and maintain consumer trust. In parallel, regulators and government authorities, including the RBI, are developing future-ready, proactive frameworks that safeguard customer interests, support fair practices, and responsible use of emerging technologies. To serve the diverse needs of 1.4 billion Indians, building a trusted ecosystem is critical.

Risk-readiness is a critical part of the industry's journey, and identifying and understanding risks is the first important step toward mitigating them. This report, the third in the series, aims to advance the collective understanding and perception of market risks. It provides market speak on the top risks and the grounds for collective action to address them. Understanding and managing these risks is essential for the industry's growth, making this study a vital resource for stakeholders towards an optimistic and secure fintech future.

Approach

The **Fintech Barometer** aims to provide a perspective on risk perception in India's fintech ecosystem. Building on previous editions, this report expands the scope beyond digital lending to encompass all fintech verticals, such as lending, payments, regtech, collection-tech, and techfins.

The findings in this report are derived through a mixed-method research approach combining quantitative survey data with qualitative stakeholder insights:

Survey

The survey was conducted by FACE and Grant Thornton Bharat and shared with FACE members and fintech leaders to capture their perspectives on key risks, sectoral challenges, innovations, and strategic recommendations shaping the Indian fintech ecosystem. Participants were asked to provide insights on nine core risk areas. The survey required participants to rank and evaluate these risks, share their experiences with operational challenges, highlight innovations driving growth, and provide recommendations to support a resilient and future-ready fintech ecosystem. The 39 fintech leaders responded to the survey between September and December 2025.
Ranks are based on weighted average severity scores assigned by survey respondents on a scale of 1–10.

Interviews

In addition to the survey, in-depth interviews were conducted with a select group of stakeholders for a wider and counter perspective.

Summary

This report presents the findings of a survey conducted by the **Fintech Association for Consumer Empowerment (FACE)** and **Grant Thornton Bharat**. Senior fintech players ranked the nine risks confronting India's fintech ecosystem on the relative severity. The findings, corroborated through select interviews reveal the risk perception among the industry. Risks are ranked based on weighted average severity scores assigned by survey respondents on a scale of 1–10.

1

Highest-rated risks are not only interrelated but also indicate that the ecosystem has reached a stage where institutional credibility, beyond innovation, plays a critical role in determining long-term sustainability. The survey highlights the sector's most significant vulnerabilities, including infrastructure risk (and the dependence on DPIs), market competition, and trust erosion among customers due to the risk of data privacy. Notably, **reputational risk emerges as the most critical category**, as it often represents the cumulative impact of breakdowns across multiple risk areas.

2

Mid-tier risks are viewed as manageable within the operating conditions that exist currently. For example, with changes in RBI's regulation-making and sharing in FY 2025-26, regulatory and governance risk appears tractable.

3

The **low-tier risks** remain a latent vulnerability. While AI/ML risk currently ranks the lowest among the nine, it reflects the relatively early stage of deployment of advanced AI use-cases and the current focus on foundational, operational and regulatory risks in the financial ecosystem and less of robust model governance. This is an important insight. In the **RBI's FREE-AI Committee Report**[1], among 171 surveyed NBFCs, only 27% were using AI in some facet of their operations. However, AI/ML and model risk will likely become a more prominent concern once advanced automation is engaged in underwriting/fraud detection/customer engagement. Moreover, macroeconomic and funding risks did not weigh in when this survey was conducted in September-December 2025. However, in the current context, this perception may be different.

Nine risks

1. Reputation and brand risk
2. Interoperability and infrastructure risk
3. Market competition and conduct risk
4. Data access, privacy and protection risk
5. Cybersecurity and business continuity risk
6. Regulatory and governance risk
7. Financial crime risk
8. Macro-economic and funding risk
9. AI/ML and model risk

A cross-cutting inference from the survey is that **most relevant or consequential risks arise outside the direct control of individual fintech firms**, as they might stem from the proliferation of unauthorised players, or the technology and fraud landscape. Furthermore, in a fast-evolving environment, perceptions and priorities regarding risks shift rapidly, which underscores the need for a Fintech Barometer to more frequently measure the pulse.

[1]RBI (2025). Framework for Responsible and Ethical Enablement of Artificial Intelligence (FREE-AI) Committee Report

Ranking risks

Overall ranking

Rank	Risk indicator	Explanation	Average rating (out of 10)
1	**Reputation and brand risk**	The risk of reputational damage, arising from negative publicity, social media backlash, perceived unethical practices, or loss of trust among key stakeholders	7.2
2	**Interoperability and infrastructure risk**	The risk of potential disruptions from failures, outages, or policy changes in India's public digital infrastructure (e.g., UPI, Aadhaar)	7
3	**Market competition and conduct risk**	The risk of potential erosion of customer base or obsolescence of business model, driven by aggressive pricing, rapid technology innovation	6.9
4	**Data access, privacy and protection risk**	The risk of potential vulnerabilities around data privacy, such as handling and protecting customer information, ensuring its security	6.6
5	**Cybersecurity, technology and business continuity risk**	The risk of potential service disruptions, financial loss, or reputational harm arising from cyberattacks (e.g., phishing)	6.5
6	**Regulatory and governance risk**	The risk of facing regulatory actions such as penalties, license suspension, or operational restrictions due to non-compliance with regulations	6.5
7	**Fraud, AML/CFT and financial crime risk**	The risk of exposure to fraudulent activities, such as identity theft, mule accounts, phishing scams, synthetic identities, or money laundering	6.3
8	**Macro-economic and funding risk**	The risk of macroeconomic changes, such as inflation, interest rate hikes, currency fluctuations, or funding slowdowns.	6.3
9	**AI/ML and model risk**	The risk of potential harm from flawed AI or machine learning models, used in areas such as credit scoring, fraud detection, marketing segmentation	5.8

01

Reputation and brand risk

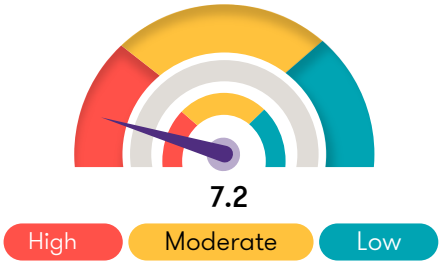
Meaning

The risk of reputational damage arising from negative publicity, social media backlash, perceived unethical practices, or loss of trust among key stakeholders.

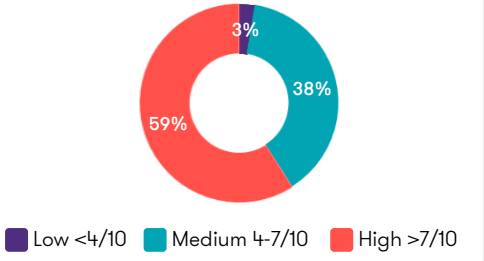
Rank

01

Average rating



Risk of reputational damage



According to survey respondents, reputational and business risks are the most severe in the market, with an average rating of **7.2 out of 10. 59% of the fintech players surveyed consider reputational damage as a high risk,** whereas **38% assessed it as a medium risk.**

A key structural challenge arises from the **absence of a universally accepted definition of a fintech entity**. Unlike banks or non-banking financial companies (NBFCs), which are established and explicitly recognised as regulated entities (REs), a wide range of digital platforms can self-identify as "fintechs" and offer digital financial services.

Digital lending illustrates this challenge, having experienced reputational spillovers: misconduct by illegal or unauthorised applications has eroded customer trust across the broader ecosystem, including compliant entities. Consequently, stakeholders, including the media and customers, often form broad, generalised perceptions of the digital lending landscape.

Efforts by the regulator, the government, FACE, and app stores to remove illegal lending apps have restored confidence, but fraudulent apps continue to target and exploit customers in novel ways, causing ongoing reputational damage.

A second dimension of reputational risk arises from the **relative newness of the fintech sector**. In contrast to traditional banking or NBFCs, where instances of non-compliance are framed as isolated lapses, individual non-compliance in the fintech ecosystem often generates sector wide scepticism. High and close public attention to the fintech sector often leads to an unusually large share of negative scrutiny and perception.

Finally, these are new-age companies catering to a very large scale of business and to the young, vociferous, digital-savvy customer segment. This means an added responsibility for high standards on privacy, customer experience, transparency, service quality, and a shortfall in meeting them leads to disproportionate reputational damage. Media amplification and public perception risks make fintechs susceptible to negative brand and reputational hits. An example is the perception of high charges or unclear fees in a price-sensitive market, which industry participants note they consistently face, despite following regulatory requirements and disclosure norms.

02

Interoperability and infrastructure risk

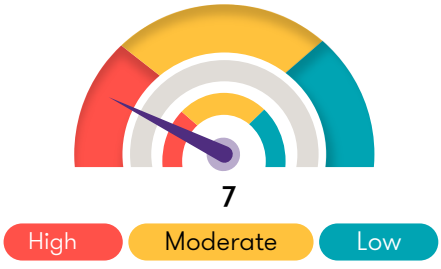
Meaning

The risk of potential disruptions from failures, outages, or policy changes in India's digital public infrastructure (e.g., UPI, Aadhaar).

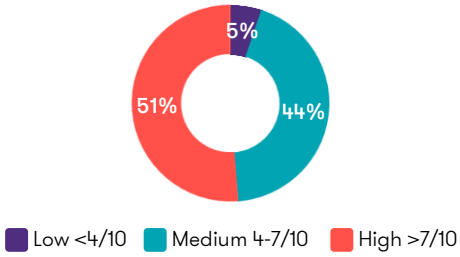
Rank

02

Average rating



Risk of failures, outages, or policy changes in DPI



As per the survey responses, **51% of the fintech players reported interoperability and infrastructure risks as high in the market**, while **44%** of players see them as medium risk, and **5%** as low risk. The average rating was **7** out of **10.**

Most fintech business models rely on shared digital infrastructure and common public rails (payment networks, identity platforms, and settlement systems) that enable interoperability across platforms. Therefore, they become susceptible to structural exposures such as technical disruptions and failures or policy changes. A high rating suggests that such exposure is perceived as an immediate concern for business continuity and not only a background dependency; it also signals that many fintech firms may still need to develop operational workarounds that partially mitigate the impact of upstream failures, thereby reducing peak dependency.

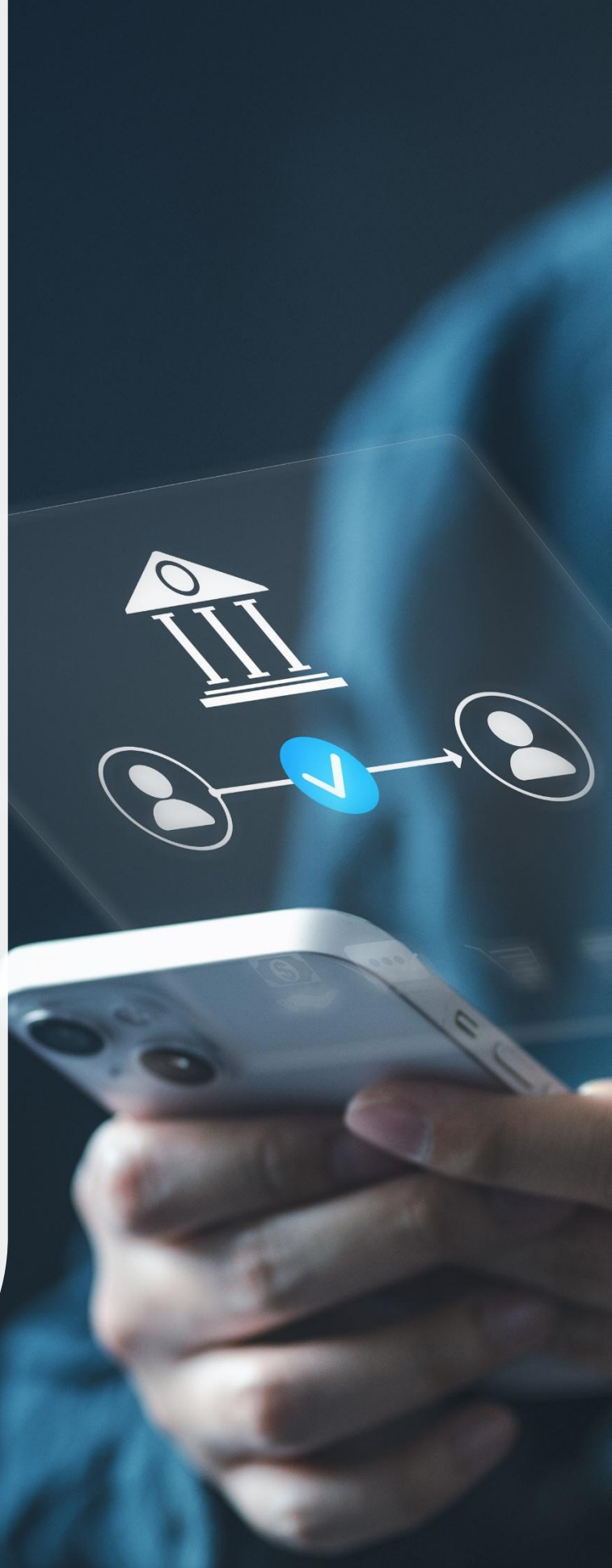
Nonetheless, India's digital payments ecosystem has benefited significantly from enabling policy measures, including the **zero-MDR framework for BHIM-UPI and RuPay debit card transactions**, which has supported large-scale adoption of digital payments. UPI's transaction value stood at INR 314.23 lakh crore in FY 2025–26, with transaction volume at around 241.6 billion, reflecting the ecosystem's depth and scale. As digital payments become increasingly central to the financial system, ecosystem participants such as payment aggregators (PAs) and third-party application providers (TPAPs) are required to make sustained investments in resilient backend infrastructure, including disaster recovery systems, multi-bank integrations, switching capacity, and reconciliation capabilities. In this context, government incentive schemes have played an important role in supporting the economics of continued infrastructure investment.

Industry participants have also emphasised the value of predictable and well-transitioned policy support, particularly for expanding digital payment acceptance in underserved geographies.

For example, the now over **Payments Infrastructure Development Fund (PIDF)**, supported the deployment of acceptance infrastructure such as QR devices, biometric tools, and soundboxes across tier-III to tier-VI markets. For fintechs involved in merchant acquisition and payment aggregation, such schemes helped offset the costs of onboarding and servicing small and micro-merchants. Continued policy support, whether through similar schemes or alternative mechanisms, can further strengthen the viability of expanding payment acceptance networks in low-density markets and contribute to broader financial inclusion objectives.

The regulator has taken concerted efforts to build resilience around dependencies that lie largely outside fintechs' direct control. DPIs developed by the Reserve Bank Innovation Hub (RBIH), including the more recent **ULI**, **MuleHunter.AI**, and the nascent **Digital Payments Intelligence Platform (DPIP)**, respectively, enable interoperable access to borrower data and provide real-time fraud detection. Unified Lending Interface (ULI), especially through its "plug-and-play" architecture, enables lenders to connect to multiple financial/non-financial data sources through a single integration layer rather than establishing multiple bilateral integrations with individual databases or service providers. This also ensures interoperability among lenders, data custodians, and other DPIs, such as AA and OCEN.

While these are welcome moves, industry participants note that certain **pre-existing DPIs may require structural upgrades to deliver similar efficiencies**; one such example is the CKYCR. Originally established to enable seamless reuse of KYC records and reduce duplication of effort, the registry may benefit from improvements in system reliability and data quality standards, according to industry participants.



03

Market competition and conduct risk

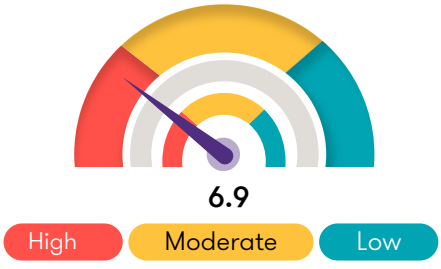
Meaning

The risk of potential erosion of customer base or obsolescence of business model driven by aggressive pricing, and rapid technology innovation.

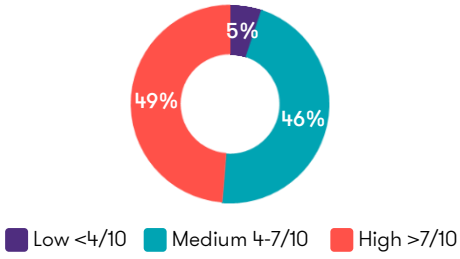
Rank

03

Average rating



Risk of erosion of customer base or obsolescence of business model



According to the survey, **market competition and conduct is perceived as high risk**, with an **average rating of 6.9**. Notably, only a meagre **5%** of the industry considers it as a low risk. The risk is a structural one, driven by the **innovation-led/competitive nature of the fintech ecosystem**, where changes in pricing, margins, or product differentiation can increase the risk of gradual erosion of market position or obsolescence if firms fail to innovate. In the case of techfins, which provides technical solutions to the BFSI sector, price competition also comes with risks of suboptimal technical solutions in terms of cyber and IT security, data protection, and operational resilience. Nonetheless, the risk is also counterbalanced by the concentration of many fintech firms within specialised market segments defined by customer profiles, distribution channels, and product verticals; this is something that provides insulation from direct price competition or rapid displacement.

In FY 2025-26, the RBI undertook several regulatory steps to set clear expectations regarding acceptable market behaviour. The **RBI (Digital Lending) Directions, 2025**[9], mandated more transparent and platform-neutral lending marketplaces by requiring comparable disclosure of loan offers and prohibiting biased ranking or dark patterns. Simultaneously, these Directions exerted a **downward rationalising pressure on lending costs** through standardised APR disclosure, prohibition of hidden/third-party charges, and the restriction on passing LSP costs to customers.

[9]RBI (2025). Digital Lending Directions, 2025

Additionally, the **RBI (Pre-payment Charges on Loans) Directions, 2025**[10], prohibited the prepayment or foreclosure charges on several floating-rate personal and MSE loans; and more recently, the **Draft RBI (NBFC – Responsible Business Conduct) Amendment Directions, 2026**[11], mandated suitability/ appropriateness assessments of financial products vis-à-vis the customer's profile, prohibited compulsory bundling, and restricted the following:

1. Incentive structures that encourage aggressive product pushing
2. Dark patterns
3. Forced consent flows

In addition, FACE as the SRO-FT keeps a close eye on the industry conduct risks and coordinates with members and regulators to address them promptly. FACE's comprehensive system consists of:

a. Setting standards;

b. Market monitoring;

c. Supporting members' compliance and capacity building with regulations and industry standards; and

d. Independent governance mechanisms to oversee and guide the SRO standards, an oversight and enforcement process (specifically addressing the market conduct risks)

[10]RBI (2025). Pre-payment Charges on Loans Directions, 2025
[11]RBI (2026). Draft RBI (NBFC – Responsible Business Conduct) Amendment Directions, 2026. *The draft was finalized and final Directions were published in June 2026 (see here).*

04

Data access, privacy, and protection risk

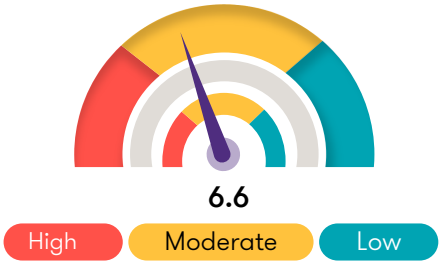
Meaning

The risk of potential vulnerabilities around data privacy, such as handling and protecting customer information, ensuring its security.

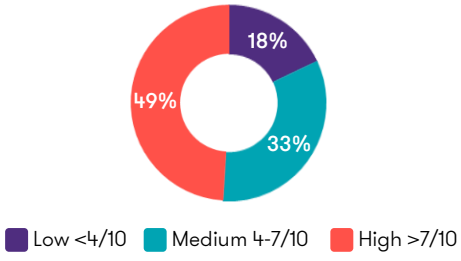
Rank

04

Average rating



Risk of data access, privacy and protection



Based on survey responses, **fintechs identified data access, privacy, and protection as moderate risk** in the fintech ecosystem, with an average severity score of **6.6.** Around **49% of respondents rated the risk as high, 33% as medium,** and only **18% as low**. This indicates data risks increasingly extend beyond compliance failures to business disruption, regulatory intervention, and reputational damage.

Where do data privacy risks emerge?

1. **Data collection:** Over-collection or non-purpose-specific consent.
2. **Data storage:** Fragmented storage across systems and vendors.
3. **Data processing:** Unauthorised secondary use (e.g., cross-selling).
4. **Data sharing:** Lack of explicit consent for third-party transfers.
5. **Data deletion:** Inability to enforce deletion across downstream systems.

Technically, privacy risks for fintechs arise from multiple sources across the digital stack; the increasing reliance on APIs, cloud infrastructure, and third-party vendors can expand the attack surface, exposing firms to unauthorised data access, system intrusions, and large-scale data breaches if vulnerabilities remain unaddressed.

Additionally, weak access controls, compromised credentials, or misconfigured servers can allow attackers to access sensitive financial and identity data.

Finally, as fintech models rely extensively on the collection of borrower data through consent-based mechanisms, they may raise concerns regarding the extent to which such consent is truly informed, explicit, and purpose-specific. There are also considerations around the potential misuse of borrowers' personal data.

Fintechs also face significant challenges in managing the data lifecycle, extending beyond collection and access risks. Personal data flows across multiple internal systems, such as loan origination systems (LOS), customer relationship management (CRM) platforms, analytics tools, as well as external vendors. This complexity makes it difficult to ensure that requests related to consent withdrawal, data deletion, or purpose limitation are consistently enforced across all downstream systems. Moreover, gaps in data discovery, particularly within unstructured environments such as employee devices or legacy databases, can inadvertently result in residual data exposure.

The regulatory landscape has evolved significantly to cope with these risks. Most notably in 2025, the Ministry of Electronics and Information Technology (MeitY) operationalised the **DPDP Act, 2023** (DPDPA)[2] by notifying the **DPDP Rules, 2025** (DPDP Rules)[3]. Together, these measures advance a consent-first architecture in India and significantly expand privacy obligations for fintech entities, now requiring them to ensure data protection compliance across product design/customer interfaces, as well as internal data management practices. Therefore, consent-related risk is now increasingly moving towards product design; under the DPDP framework, poorly designed consent architecture (bundled consents, pre-checked boxes, or lack of purpose-specific disclosures) can render consent invalid. Additionally, fintechs offering a suite of products face the add-on complexity of distinguishing between 'platform-level' and 'product-level' consent.

The DPDP Rules also introduce operational obligations, such as mandatory breach reporting within defined timelines, the implementation of security safeguards, and the maintenance of data logs to detect breaches. Moreover, certain entities classified as significant data fiduciaries (SDFs) may be required to conduct periodic data protection impact assessments and implement enhanced technical safeguards, thereby further raising compliance thresholds for larger fintechs.

It must be noted that data privacy risks are closely intertwined with reputational exposure, and these risks may rise amid heightened public scrutiny due to allegations of data misuse and a lack of informed consent.

[2]MeitY, Government of India (2023). Digital Personal Data Protection Act, 2023
[3]MeitY, Government of India (2025). Digital Personal Data Protection Rules, 2025

05

Cybersecurity, technology, and business continuity risk

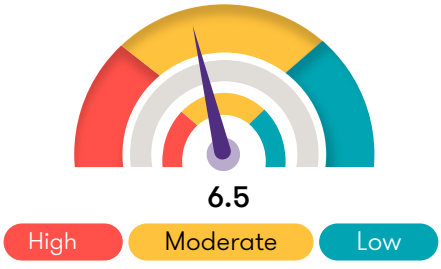
Meaning

The risk of potential service disruptions, financial loss, or reputational harm arising from cyberattacks (e.g., phishing).

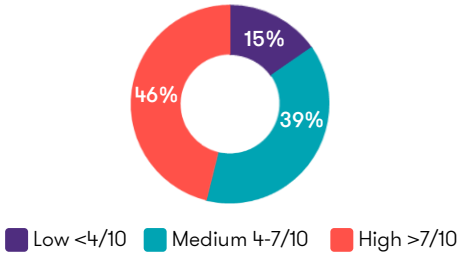
Rank

05

Average rating



Risk from cyber attacks



As per the survey, **fintech players rated cybersecurity, technology, and business continuity risks as moderate, with an average score of 6.5.** While **46%** viewed the risk as highly severe, **39%** viewed the risk as moderately severe, while only **15%** considered it low, reflecting persistent structural vulnerabilities across the ecosystem.

Because fintech players increasingly rely on cloud infrastructure, mobile applications, APIs, and third-party service providers, they are inherently exposed to cyber threats (such as phishing, malware, ransomware, distributed denial-of-service attacks, and system intrusions), as well as operational risks arising from software defects, infrastructure failures, or vendor outages. According to RBI data[13], **the average cost of a data breach reached ~USD 2.18 million in 2023 in India**, with the **most common attack being phishing**, followed by stolen/ compromised credentials. These threats are now increasingly being amplified by AI, which enables highly personalised fraud (e.g., deepfakes).

However, the moderate rating suggests that respondents generally do not view these threats as an immediate existential risk to ongoing operations; notwithstanding this confidence, the underlying exposure remains significant, and regulators have emphasised the need for robust and resilient cyber and IT security and oversight of technology risk.

[13]RBI (2024). Report on Currency and Finance 2023-24

06

Regulatory and governance risk

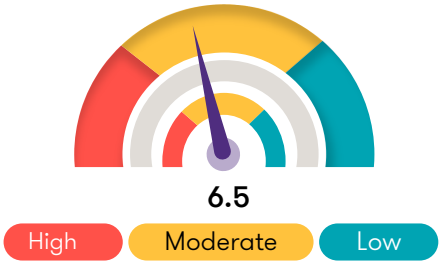
Meaning

The risk of facing regulatory actions such as penalties, license suspension, or operational restrictions due to non-compliance with regulations.

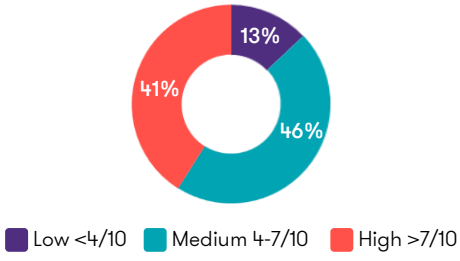
Rank

06

Average rating



Risk of regulatory actions and non-compliance



Based on survey responses, **41% of fintech players rated regulatory and governance risk as high, 46%** as moderate, and **13%** as low, leading to an **average risk score of 6.5 out of 10.** Importantly, even respondents who classified the risk as "moderate" observed that regulatory responses to compliance gaps may extend beyond monetary penalties and can, in some cases, affect onboarding, product operations, or partner arrangements. This highlights the need for proactive compliance management and timely remediation.

A recent and notable example of such business disruption occurred in November 2025, when **SEBI issued a public advisory cautioning investors about "digital gold" products offered by online platforms**[4]. The transaction value of digital gold increased nearly threefold between January and December 2025[5], prompting SEBI to highlight the potential counter-party and operational risks associated with such arrangements and clarify that these products fell outside its regulatory ambit.

This case illustrates how fintech innovation (particularly that which does not align neatly with existing regulatory frameworks) can be exposed to regulatory risks that may constrain growth. It also reflects the evolving distinction between fintech entities and traditional financial institutions that operate within more stable regulatory environments. Furthermore, fintech innovation (often characterised by complex structures that combine regulated and unregulated activities, outsourcing arrangements, technology platforms, and partner-led delivery models)can blur accountability, complicate compliance management, and, at times, create ambiguity regarding regulatory jurisdiction.

Supervisory measures affecting fintechs include costs associated with third-party risk assessments and onboarding restrictions, product suspensions, limitations on specific activities, directives to modify business practices, and constraints on business expansion. It must be noted that, since fintechs depend on REs for partnership, such supervisory action can cascade downstream across the value chain. However, in the past few years, compliance and governance have taken centre stage as key to growing and scaling sustainably. As many fintechs grow, become more regulated, more integrated with REs, and listed, there is a high degree of attention to governance and compliance.

[4]SEBI (2025). Caution to public regarding dealing in 'Digital Gold'
[5]World Gold Council (2026). India gold market update: Enduring demand strength

From the regulator's standpoint, such interventions represent a corrective/preventive approach aimed primarily at safeguarding consumers' interests.

The regulator has taken steps to mitigate the risk of inadvertent non-compliance on the part of fintechs also. To streamline compliance, the RBI, in November 2025, carried out a **major consolidation of its regulatory instructions by reorganising more than 9,000 circulars, guidelines, and directions administered by its Department of Regulation (RBI-DoR)** into nearly 240 function-wise Master Directions covering 11 categories of REs[6]. In addition, in 2025, the RBI, through its **Framework for Formulation of Regulations[7],** streamlined the process of issuing new regulations.

A well-received development in this framework was its decision to release a general statement outlining its response to the feedback received when finalising the regulation.

Such a measure, by providing a clear rationale for regulation, brings industry on board with a collective public policy objective. In addition, other efforts by the RBI, such as monthly events like Finquiry and Finteract, and recognition of the **self-regulatory organisation in the fintech sector** (SRO-FT), provide a platform to fintechs to develop a collective understanding of evolving regulatory and supervisory directions.

Interoperability in financial innovation is also aided by the **Interoperable Regulatory Sandbox (IoRS)[8]**, which facilitates the testing of innovative products/services that fall under the regulatory ambit of multiple financial-sector regulators, such as, the RBI, SEBI, IRDAI, IFSCA and PFRDA. True to its name, the interoperable sandbox opens up avenues for the controlled testing and regulatory approval of cross-sectoral financial products.

[6]RBI Press Release (2025). *Reserve Bank of India issues Consolidated Master Directions*
[7]RBI (2025). *Policy Statement: Framework for Formulation of Regulations*
[8]RBI FAQ (2025). *Inter-operable Regulatory Sandbox (IoRS)*

07

Fraud, AML/CFT, and financial crime risk

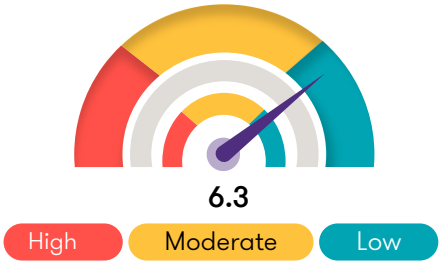
Meaning

The risk of exposure to fraudulent activities such as identity theft, mule accounts, phishing scams, synthetic identities, or money laundering.

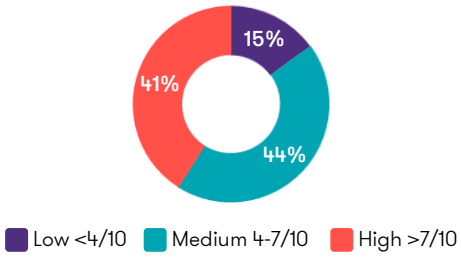
Rank

07

Average rating



Risk of fraudulent activities and financial crimes



According to the survey, **financial crime risk is perceived as low risk** with an average rating of **6.3.** Among the fintech players **41%** reported the risk of fraudulent activities and financial crimes as severe in the market, while **44s%** assessed it as medium risk, and **15%** considered it low risk.

Digital fraud has been flagged as a growing national concern by the regulators and government authorities, especially in the context of India's expanding financial ecosystem. This is because digital financial services can carry heightened fraud risk due to remote onboarding, real-time transaction processing, identity misuse, account takeover risks, and social engineering-led frauds. The risk posed by the latter, especially identity theft and synthetic accounts, has compelled the industry to regularly update and invest in digital KYC solutions. From a regulatory intervention standpoint, India's response to identity misuse and mule-account activity has focused on strengthening customer risk management. The RBI's framework already requires REs to undertake risk-based customer due diligence, verify identity through prescribed channels, periodically update KYC records, and subject higher-risk accounts to enhanced monitoring. In parallel, supervisory emphasis has increased on post-onboarding controls, including the detection of unusual account behaviour, the filing of suspicious transaction reports, and the monitoring of accounts that may be used as conduits for fraud proceeds.

Furthermore, the recent **TRAI intervention on mandating the 1600-series numbering system and tighter unsolicited commercial communication (UCC)** controls seek to improve the authenticity and traceability of BFSI calls and messages, reducing impersonation, phishing, and KYC-related fraud risks. The **RBI's proposed 2026 Amendment Directions for Review of Framework of Limiting Customer Liability in Digital Transactions** [12] complement this by addressing post-fraud outcomes through broader coverage, faster complaint resolution, and structured compensation for small-value digital payment frauds.

Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT)

[12]RBI (2026). Draft Amendment Directions for 'Review of Framework of Limiting Customer Liability in Digital Transactions'

08

Macro-economic and funding risk

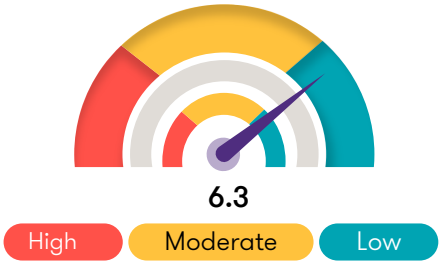
Meaning

The risk of macroeconomic changes such as inflation, interest rate hikes, currency fluctuations, or funding slowdowns.

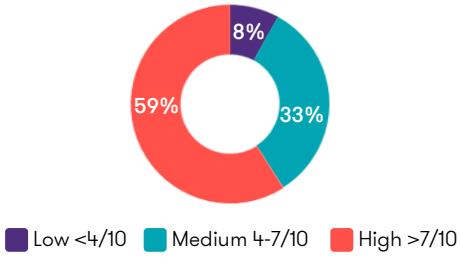
Rank

08

Average rating



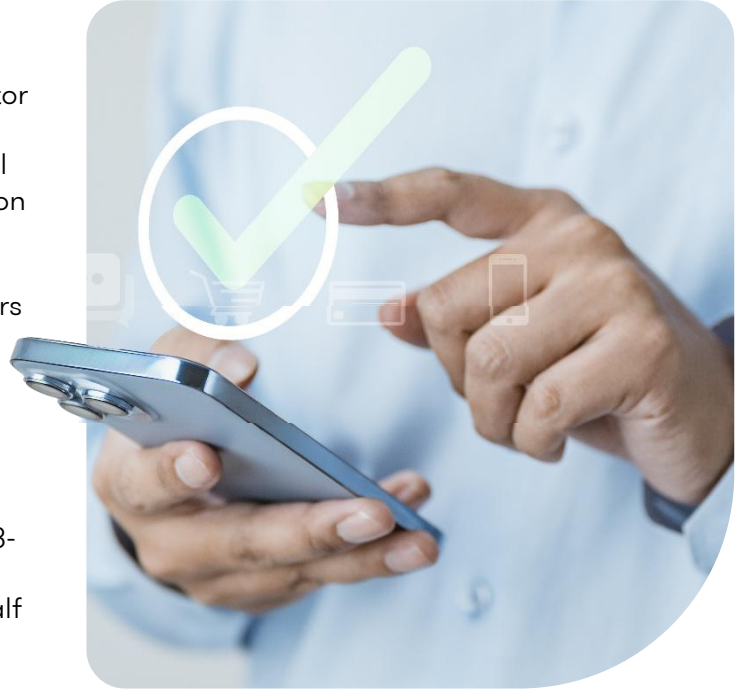
Risk from macroeconomic changes



Fintech businesses consider the risk arising out of inflation, interest rate hikes, currency fluctuations, or funding slowdowns as low with an average rating of 6.3. Among the fintech players, **59%** assessed the risk as high whereas **33%** considered the risk as moderate and only **8%** assessed it as a low risk.

Although the total startup funding in India declined YoY in 2025, **fintech attracted approximately USD 2.5 billion in funding, emerging as the highest-funded sector**[14]. Investor interest in fintech is concentrated in credit-led fintechs, payments infrastructure, and financial platforms aligned with India's rising consumption and credit demand. While deal volumes have fallen, average ticket sizes have increased significantly. These might be contributing factors to respondents' rating macroeconomic and funding risk as low, suggesting that broad economic conditions are not perceived as an immediate constraint on operations or growth.

From a macroeconomic standpoint[15], India estimates a real GDP growth in the range of 6.8-7.2% for FY 2026-27. With monetary conditions supportive (repo rate at 5.25% as of the first half of 2026) and inflation averaging 1.7% in April-December 2025, macroeconomic risk is viewed more as a background/ contextual factor affecting both valuations and growth trajectories in the long term than as an immediate operational risk. In general, fintech organisations remain highly optimistic about India's growth potential and see the segment as a strategic pillar to support and benefit from inclusive growth.



[14] https://www.rbi.org.in/scripts/BS_PressReleaseDisplay.aspx?prid=63011
[15] Ministry of Finance, Government of India (2026). Economic Survey 2025-26

09

AI/ML and model risk

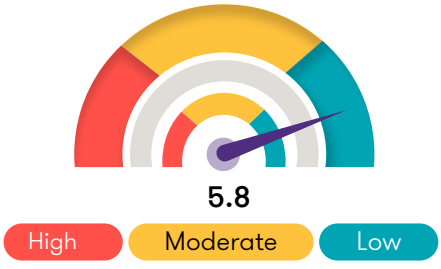
Meaning

The risk of potential harm from flawed AI or machine learning models — used in areas such as credit scoring, fraud detection, marketing segmentation.

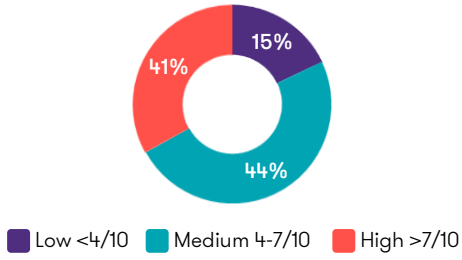
Rank

09

Average rating



Risk from AI and ML models



As per the survey responses, fintech players provided an **average rating of 5.8 to risks arising from AI and ML models. 44%** of fintech players assessed the risk as moderate, **41%** as high, and only **15%** as low.

The reason for such a low-risk rating is partially because as corroborated by surveys under the **RBI FREE-AI Committee Report[16], AI adoption in BFSI remains low, and is restricted to larger institutions and relatively simple models that require both low investment and infrastructure** (including customer support, sales and marketing, credit underwriting, and cybersecurity, in that order). In fact, only 27% of surveyed NBFCs had adopted AI in some aspect of their operations.

There is some merit to the low-risk assessment; however, the surveys also note that entities are keen to explore Generative AI (GenAI) use cases, as well as AI's potential to expand financial services to underserved and unserved populations. This rating is also attributed to entities' uncertainty in applying AI to advance use cases, given its inherent opaqueness, unpredictability, and associated challenges of governance.

Within the FREE AI Report surveys, entities identified data privacy, cybersecurity, governance, and reputational loss as the top risks associated with AI. Notably, only a quarter of respondents had established formal processes to mitigate AI-related incidents or failures, and a majority lacked a policy dedicated to training AI models.

[16]RBI (2025). FREE AI Committee Report (p. 25-33)

Conclusion

1 Sector maturity and shifting priorities

The Fintech Barometer highlights the sector entering a more mature phase of development. The earlier emphasis on speed, access and product innovation is now being complemented by a stronger focus on resilience, governance and customer trust. This shift is evident in how industry participants assess risk. The most significant concerns are no longer isolated operational issues but systemic vulnerabilities that could undermine confidence in the wider ecosystem. Fintechs are, therefore, increasingly evaluated not only on their ability to scale, but also on the robustness of their controls, conduct and institutional readiness.

2 Interconnected nature of risk

A key insight from the study is that **risk in the fintech ecosystem is inherently interconnected**. Weaknesses in areas such as interoperability and infrastructure dependence, data protection, fraud controls, governance, or third-party oversight can quickly translate into reputational damage. This is particularly relevant in a sector characterised by high transaction volumes, heavy reliance on digital channels, and a large, diverse customer base. As fintechs deepen their presence across credit, payments, wealth, insurance, collections and regulatory technology, the tolerance for control gaps is expected to diminish. Consequently, firms will need to move beyond minimum compliance and adopt a more integrated and forward-looking approach to risk management.

3 Evolving regulatory and policy environment

The evolving risk landscape is being matched by a responsive policy and regulatory environment that seeks to balance innovation with accountability and customer protection. Recent developments across digital lending, data protection, payment systems, fraud mitigation and responsible conduct indicate a clear intent to strengthen oversight while enabling continued innovation. Importantly, many fintech risks extend beyond the boundaries of individual firms, emerging from complex networks of partnerships, shared infrastructure and digital distribution channels.

4 Implications for fintech firms

For the fintech firms, the implications are clear. Continued growth will depend on embedding strong governance frameworks early in the business lifecycle, rather than treating them as a later-stage requirement. This includes establishing effective board and management oversight, ensuring accountability for partner-led activities, strengthening data and consent management, enhancing grievance redress mechanisms, and building robust cyber and fraud risk capabilities. Emerging risks, such as those related to AI models and funding, may appear less immediate but are likely to gain prominence as business models scale and complexity increases.

5 Need for ecosystem collaboration and long-term growth

The findings highlight that India's fintech future will depend on collaborative action across regulators, institutions and technology players. Strengthening standards, information sharing and risk management, while balancing innovation with responsibility, is vital to build trust, ensure security, advance inclusion and drive sustainable, long-term ecosystem growth.

Acknowledgements

Grant Thornton Bharat

Rohan Lakhiyar
Partner, Financial Services Risk Advisory

Yogesh Purohit
Director, Financial Services Risk Advisory

FACE

Sugandh Saxena
CEO, FACE
E: sugandh@faceofindia.org

Saishya Duggal
Manager - Policy and Research, FACE
E: saishya.duggal@faceofindia.org

Contributors:

Mohit Mathur
Director, Market Ecosystems

Aakriti Malik
Assistant Manager, Market Ecosystems

Gayatri Gola
Consultant, Global Research Centre

Editorial review	Design
Runa Dasgupta	Roshani Kumari

For media enquiries, write to

media@in.gt.com

About FACE

The **Fintech Association for Consumer Empowerment (FACE)** is the RBI-recognised Self Regulatory Organisation in the Fintech Sector (SRO-FT). Fintech companies of all kinds come together at FACE to build an industry that delivers customer-centric financial services that are safe, suitable, and transparent—driving real impact across society and the economy.

As Fintech continues to expand, FACE provides the institutional platform to guide its growth. We unite providers, enablers, and stakeholders in a shared commitment to responsible innovation. Through our work across standards-setting, compliance, governance, consumer protection, and industry advocacy, FACE is shaping a resilient and trusted Fintech ecosystem for India.

FACE membership includes 390+ institutions across India's Fintech ecosystem.

#ResponsibleFintech
#EmpoweredConsumers

About Grant Thornton Bharat

At Grant Thornton Bharat, we are committed to bringing positive change to all that we do. We are a founding member firm of the Grant Thornton international network and India's pre-eminent consulting firm. We offer a range of solutions in assurance, tax, technology, managed services, deals, ESG and risk consulting to mid-market companies, government, large corporates, and digital natives. We **#GoBeyond** for our people, clients, and communities to shape **Vibrant Bharat.**

22 offices | 13,000+ people

Part of Grant Thornton International:
80,000+ people | 150+ countries

Our offerings

Our offerings include solutions for governments, large corporates, middle market and digital natives across various industries and channels:

- **Assurance**
- **Global delivery**
- **Deals consulting**
- **Tax, regulatory & finance consulting**
- **ESG & risk consulting**
- **Transformation consulting**

TIME INDIA'S BEST EMPLOYERS statista 2025

Great Place To Work® Certified NOV 2025–NOV 2026 INDIA ™

Best Workplaces™ in Professional Services Great Place To Work. INDIA 2025

We are
Shaping Vibrant Bharat

A member of Grant Thornton International Ltd., Grant Thornton Bharat is at the forefront of helping reshape the values in the profession. We are helping shape various industry ecosystems through our work across Assurance, Tax, Risk, Transactions, Technology and Consulting, and are going beyond to shape a more **#VibrantBharat.**

Our offices in India

● Ahmedabad ● Bengaluru ● Bhubaneswar ● Chandigarh ● Chennai
● Dehradun ● Gandhinagar ● Goa ● Gurugram ● Guwahati ● Hyderabad
● Indore ● Jaipur ● Kochi ● Kolkata ● Mumbai ● New Delhi ● Noida ● Pune

Scan QR code to see our office addresses
www.grantthornton.in

Connect with us on

@Grant-Thornton-Bharat-LLP
@GrantThorntonBharat
@GrantThornton_Bharat
@GrantThorntonIN
@GrantThorntonBharatLLP
GTBharat@in.gt.com

17574 | RD | RK