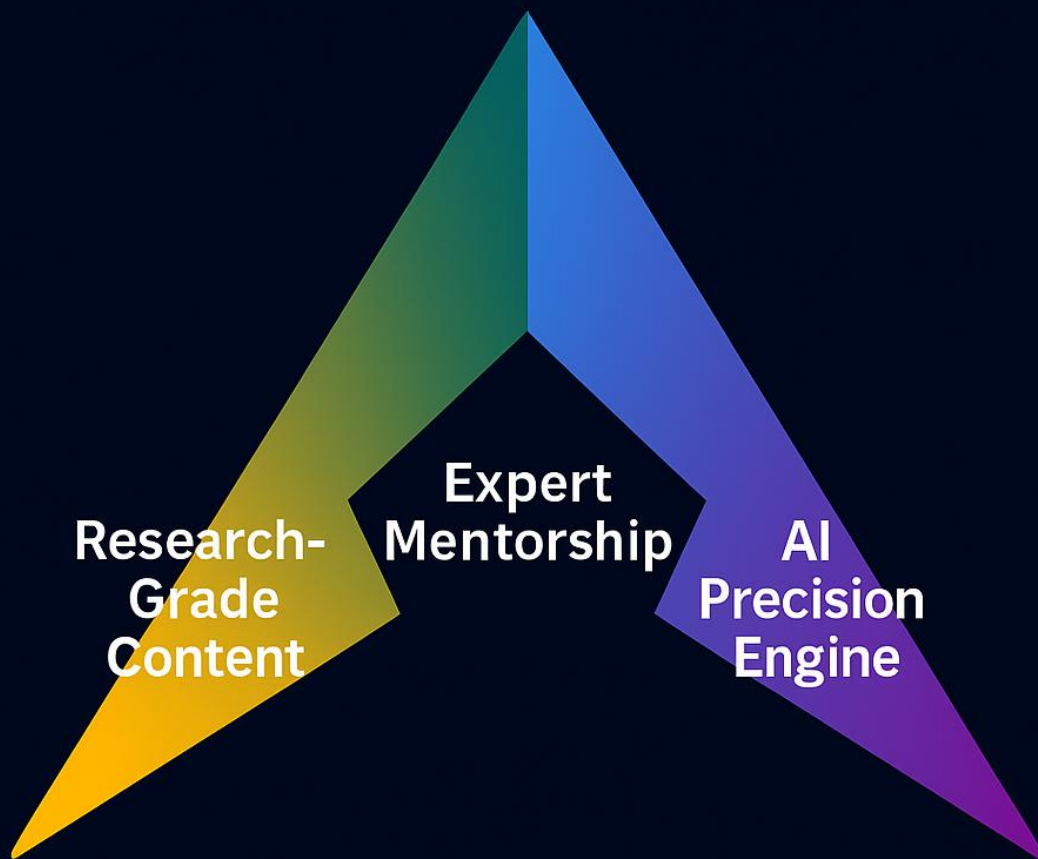


PrepAlpine

The Next-Generation UPSC Institution

Where Research Meets Mentorship & Precision



Preparation Meets Precision

A Next-Generation Learning Institution

Copyright © 2025 PrepAlpine

All Rights Reserved

No part of this publication may be reproduced, distributed, or transmitted in any form or by any means—whether photocopying, recording, or other electronic or mechanical methods—without the prior written permission of the publisher, except in the case of brief quotations embodied in critical reviews and certain non-commercial uses permitted by copyright law.

For permission requests, please write to:

PrepAlpine

Email: info@PrepAlpine.com

Website: PrepAlpine.com

Disclaimer

The information contained in this book has been prepared solely for educational purposes. While every effort has been made to ensure accuracy, PrepAlpine makes no representations or warranties of any kind and accepts no liability for any errors or omissions. The use of any content is solely at the reader's discretion and risk.

DAILY CURRENT AFFAIRS DATED 30.06.2026

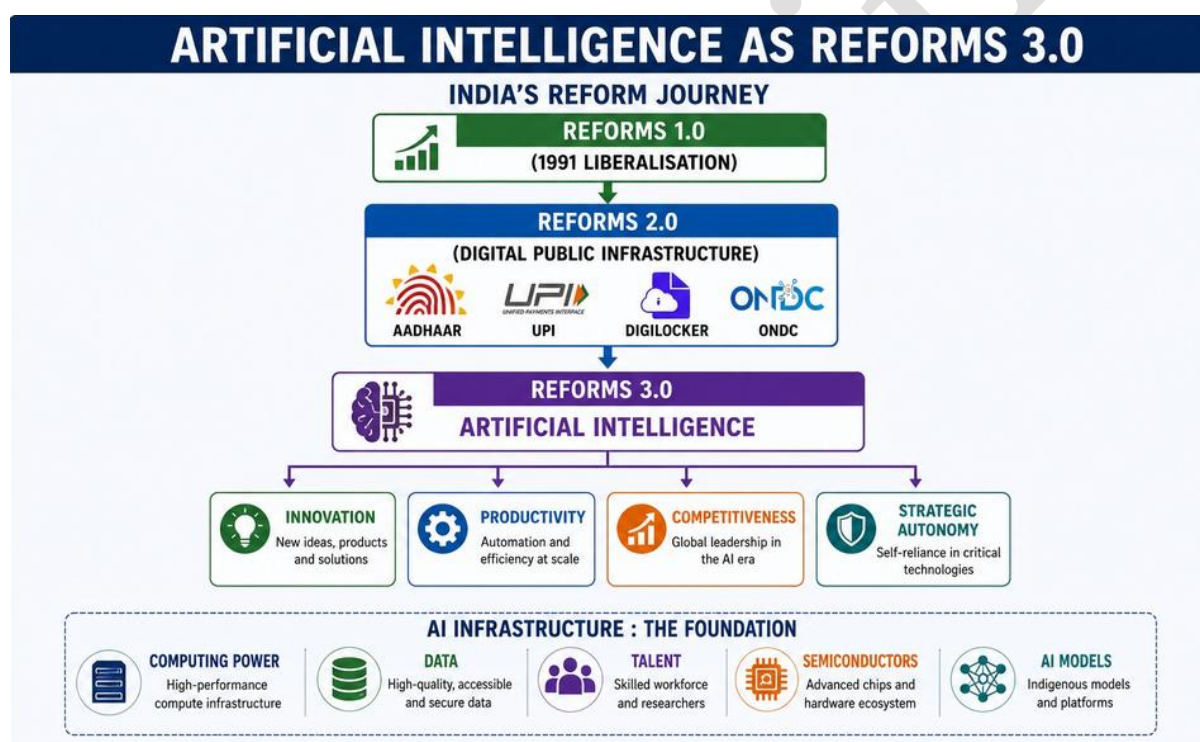
GS Paper III: Economics

1. Artificial Intelligence as "Reforms 3.0": Building India's AI Infrastructure

a. Introduction

Artificial Intelligence (AI) is emerging as a foundational technology capable of transforming productivity, innovation and economic competitiveness across virtually every sector of the economy. Much like the 1991 economic reforms integrated India into the global economy and the Digital Public Infrastructure (DPI) revolution transformed digital governance, AI has the potential to drive the next phase of India's structural transformation.

Against this backdrop, AI should be viewed as "Reforms 3.0", requiring sustained investment in sovereign AI infrastructure, open-source innovation and affordable computing resources. The broader policy objective is to strengthen India's technological competitiveness while ensuring strategic autonomy in an increasingly AI-driven world.



b. Background Context

Artificial Intelligence has become a strategic technology underpinning economic growth, national security and technological leadership. Countries are increasingly competing to develop advanced AI capabilities by investing in computing infrastructure, high-quality datasets, semiconductor ecosystems and skilled human resources.

India has already established globally recognised Digital Public Infrastructure (DPI) through initiatives such as Aadhaar, Unified Payments Interface (UPI), DigiLocker and the Open Network for Digital Commerce (ONDC). However, continued dependence on foreign AI models, cloud infrastructure and advanced computing hardware presents challenges for long-term technological self-reliance.

While India possesses a strong digital foundation, several structural constraints continue to limit its emergence as a global AI leader.

c. Key Issues

Low Investment in Research and Development

- India's expenditure on Research and Development (R&D) remains around 0.65% of GDP, considerably lower than major innovation-driven economies.
- Limited investment constrains indigenous technology development and frontier scientific research.

Dependence on Foreign AI Ecosystems

- Heavy reliance on foreign AI models, cloud platforms and computing infrastructure.
- Creates concerns relating to technology sovereignty, strategic autonomy and supply-chain resilience.
- External dependence may expose critical sectors to geopolitical or commercial disruptions.

Limited Access to High-Performance Computing

- Advanced computing infrastructure remains prohibitively expensive.
- Universities, research institutions, startups and MSMEs often lack affordable access to AI computing resources.
- Unequal access widens technological disparities within the innovation ecosystem.

These structural limitations underline why AI is increasingly viewed not merely as a technology sector but as a strategic economic capability.

d. Why Artificial Intelligence is Strategically Important

Driver of Productivity and Economic Growth

- Improves efficiency across healthcare, agriculture, manufacturing, logistics, education, finance and public administration.
- Reduces operational costs and enhances service delivery.

Foundation of the Digital Economy

- Accelerates innovation.
- Supports knowledge-intensive industries.
- Creates new opportunities for entrepreneurship and high-skilled employment.

Strategic Autonomy

- Indigenous AI capabilities reduce dependence on foreign technology providers.
- Strengthen national security, technological sovereignty and data governance.
- Enable AI solutions tailored to India's developmental priorities.

Strengthening Digital Public Infrastructure

- AI enhances citizen-centric governance built upon Aadhaar, UPI, DigiLocker and ONDC.
- Facilitates intelligent public services and data-driven policymaking.

Realising these strategic advantages requires focused policy interventions aimed at building domestic AI capabilities.

e. Policy Priorities

Build Sovereign AI Infrastructure

- Develop domestic high-performance computing capacity.
- Support indigenous training and deployment of large language models (LLMs).

- Reduce strategic dependence on external computing infrastructure.

Promote Open-Source AI

- Encourage development of open-source AI models.
- Reduce reliance on proprietary foreign platforms.
- Foster collaborative research and innovation.

Diversify AI Infrastructure

- Avoid excessive dependence on a single cloud or hardware provider.
- Improve resilience through diversified computing ecosystems.
- Enhance long-term technological competitiveness.

Democratise Access to Computing Resources

- Expand affordable computing access for universities, startups and research institutions.
- Promote well-designed Public-Private Partnerships (PPPs) to strengthen AI infrastructure.

Strengthen the Innovation Ecosystem

- Increase investment in R&D.
- Develop AI talent through higher education and skill development.
- Promote interdisciplinary collaboration among academia, industry and government.

While these priorities provide a roadmap for AI leadership, their implementation faces important structural and technological challenges.

f. Key Challenges

High Capital Requirements

Building AI infrastructure requires substantial investment in:

- Data centres.
- High-performance computing.
- Energy infrastructure.
- Skilled human resources.

Rapid Technological Change

- AI capabilities evolve faster than regulatory frameworks and institutional capacity.
- Long-term infrastructure planning becomes increasingly complex.

Semiconductor Dependence

- India remains dependent on imported semiconductors, GPUs and advanced processors.
- Limits complete technological self-reliance.

Balancing Innovation and Regulation

- Excessive regulation may discourage innovation.
- Weak governance may create risks relating to privacy, security and misuse.
- Policy must balance openness, innovation, national security and data protection.

Addressing these challenges requires coordinated investments, institutional reforms and long-term strategic planning.

g. Way Forward

Increase Investment in AI

- Expand both public and private investment in AI research and innovation.
- Strengthen advanced computing infrastructure.

Accelerate the IndiaAI Mission

- Build indigenous computing capacity.
- Develop high-quality datasets.
- Strengthen AI research institutions and skilled human resources.

Foster Collaborative Innovation

- Encourage partnerships among government, academia, startups and industry.
- Promote knowledge sharing and technology transfer.

Develop Responsible AI Governance

- Establish transparent, accountable and ethical AI governance frameworks.
- Ensure responsible innovation while protecting public interest.

Strengthen Strategic Technology Ecosystems

- Expand domestic semiconductor manufacturing.
- Invest in high-performance computing.
- Build resilient digital infrastructure supporting long-term technological sovereignty.

h. Global Perspective

Major economies are treating AI infrastructure as a strategic national asset.

- **United States:** Investing heavily in frontier AI research, advanced chips and private-sector innovation.
- **European Union:** Combining AI innovation with a risk-based regulatory framework through the EU AI Act.
- **China:** Pursuing state-supported AI development alongside domestic semiconductor manufacturing and computing infrastructure.
- **Japan and South Korea:** Expanding investments in AI, advanced computing and semiconductor resilience.

India's AI strategy must therefore balance innovation, strategic autonomy and global competitiveness while leveraging its strengths in Digital Public Infrastructure and software capabilities.

Conclusion

Artificial Intelligence has the potential to become the next major driver of India's economic transformation, much as the 1991 reforms reshaped the country's growth trajectory and Digital Public Infrastructure revolutionised governance. Achieving this vision, however, requires sustained investment in sovereign AI infrastructure, research and innovation, semiconductor capabilities and skilled human capital. A balanced strategy that combines technological self-reliance, responsible governance and global collaboration will be essential for positioning India as a leading AI-powered economy while preserving its strategic autonomy.

GS Paper III: Security

2. Reserve Bank of India's Revised Compensation Framework for Digital Payment Frauds

a. Introduction

India's rapid expansion of digital payments has transformed financial inclusion, convenience and the delivery of banking services. Platforms such as the Unified Payments Interface (UPI), internet banking and mobile banking have made digital transactions an integral part of daily economic activity. However, this rapid digitalisation has also led to a sharp increase in sophisticated cyber frauds that exploit both technological vulnerabilities and human behaviour.

Recognising this evolving threat landscape, the Reserve Bank of India (RBI) has issued revised directions on customer liability and compensation for digital payment frauds. The new framework expands regulatory protection beyond conventional unauthorised electronic transactions to include frauds involving social engineering, coercion and stolen credentials. The revised directions will be implemented on a pilot basis from 1 January 2027.

b. Background Context

India's digital payment ecosystem has expanded rapidly over the past decade, driven by the growth of UPI, internet banking, mobile banking and digital wallets. While these innovations have improved financial inclusion and ease of transactions, cybercriminals have simultaneously adopted increasingly sophisticated fraud techniques.

The RBI's 2017 framework primarily addressed unauthorised electronic transactions arising from technical breaches such as hacking or system compromise. However, recent frauds increasingly rely on social engineering, where victims are deceived into voluntarily authorising transactions through manipulation, impersonation or intimidation. The revised framework seeks to address these emerging risks.

The revised directions therefore represent a significant shift from protecting customers only against technical breaches to recognising behavioural manipulation as a major cyber security challenge.

c. Key Changes in the Revised Framework

Expanded Coverage of Fraud

The revised framework extends protection to fraudulent electronic banking transactions arising from multiple circumstances.

It now includes:

- Fraudulent acquisition of customer credentials through phishing, impersonation, fake customer care calls and other forms of social engineering.
- Transactions carried out under coercion or duress, including scams such as digital arrest frauds.
- Certain losses arising from negligence by banks or third parties, subject to RBI-prescribed conditions.

Shift from the Earlier Framework

The 2017 framework largely focused on transactions that were completely unauthorised by customers.

The revised framework recognises that customers may sometimes authorise payments only because they have been deceived or coerced, thereby expanding the scope of consumer protection.

Along with broader eligibility, the RBI has also introduced a structured compensation mechanism designed to balance customer protection with responsible reporting.

d. Compensation Framework

Compensation Amount

- Eligible customers suffering losses of up to ₹50,000 may receive compensation equal to 85% of the loss, subject to a maximum compensation of ₹25,000.

Lifetime Benefit

- Compensation is available once during the customer's lifetime, provided all prescribed eligibility conditions are fulfilled.

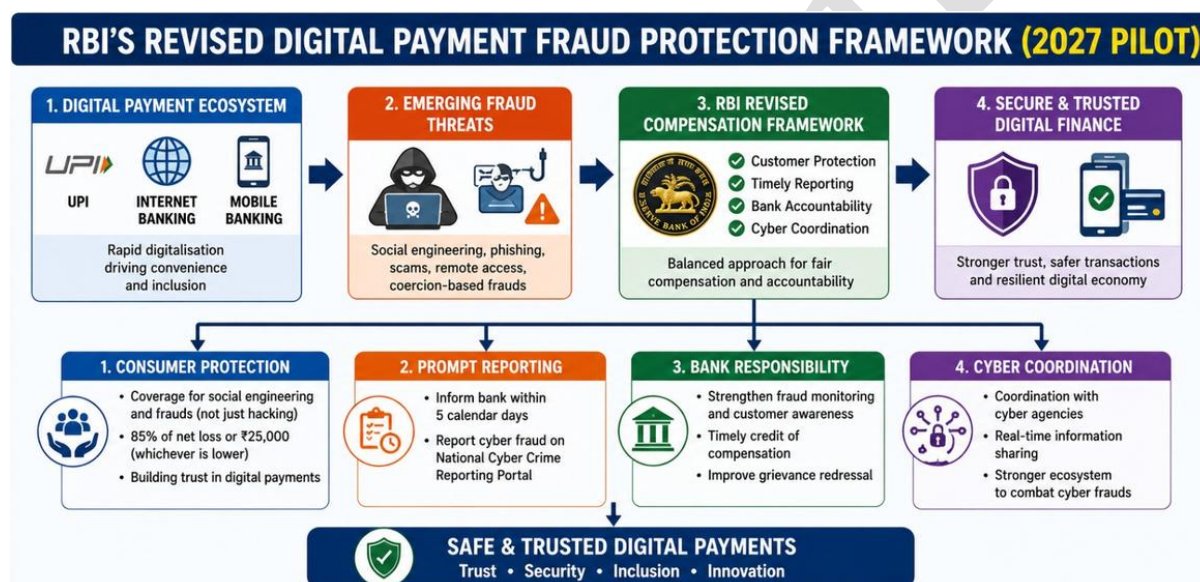
Mandatory Reporting

- Customers must report the fraud through the National Cyber Crime Helpline (1930) within five calendar days of the fraudulent transaction.
- Procedural requirements specified by the RBI must also be satisfied.

Zero Customer Liability After Reporting

- Once a customer reports the fraud, any subsequent fraudulent electronic banking transaction attracts zero customer liability.
- This prevents additional financial losses after timely reporting.

Beyond compensation, the revised framework has broader implications for digital financial inclusion and cyber security governance.



e. Significance of the Revised Framework

Recognising the Changing Nature of Cybercrime

- Modern digital frauds increasingly depend on social engineering, impersonation and psychological manipulation rather than direct hacking.
- The revised framework aligns banking regulation with contemporary cybercrime patterns.

Strengthening Consumer Confidence

- Improved customer protection enhances trust in digital payment systems.
- Greater confidence supports wider adoption of digital financial services and advances financial inclusion.

Encouraging Prompt Reporting

- Linking compensation with timely reporting incentivises customers to report fraud immediately.
- Early reporting improves the chances of freezing fraudulent transactions and tracing illicit fund flows.

Improving Institutional Coordination

- Encourages closer cooperation among banks, payment service providers and cybercrime agencies.
- Strengthens the overall digital financial security ecosystem.

While the revised framework marks an important regulatory advancement, several implementation challenges remain.

f. Key Challenges

Limited Compensation Coverage

- The framework currently applies only to relatively small-value frauds.
- Victims of larger financial losses remain outside its scope.

Reporting Timeline

Mandatory reporting within five days may disadvantage:

- Elderly persons.
- Digitally less-literate individuals.
- Rural users.
- Vulnerable sections that may not immediately recognise fraud.

Limited Public Awareness

Many customers remain unaware of:

- The National Cyber Crime Helpline (1930).
- Reporting procedures.
- Eligibility conditions.

Lack of awareness may prevent eligible victims from obtaining compensation.

Emerging Nature of Cyber Fraud

- Fraud techniques evolve rapidly.
- Regulatory frameworks require continuous review to remain effective.

Addressing these limitations will require stronger consumer awareness, technological safeguards and adaptive regulatory mechanisms.

g. Way Forward

Review the Pilot Framework

- Periodically assess implementation outcomes.
- Expand customer protection based on operational experience and emerging fraud trends.

Strengthen Digital Financial Literacy

- Conduct nationwide awareness campaigns.
- Educate citizens regarding common cyber fraud techniques.
- Promote awareness of reporting mechanisms such as 1930 and the National Cyber Crime Reporting Portal.

Improve Fraud Detection

- Invest in AI-enabled fraud detection systems.

- Strengthen real-time transaction monitoring.
- Use behavioural analytics to identify suspicious transactions before financial losses occur.

Enhance Institutional Coordination

- Strengthen collaboration among the RBI, banks, payment system operators and cybercrime agencies.
- Improve investigation, fund recovery and customer support mechanisms.

Periodically Revise Compensation Norms

- Review compensation limits and eligibility conditions in light of evolving digital payment volumes and cyber risks.
- Ensure that customer protection keeps pace with technological change.

h. Comparison: RBI Framework 2017 vs Revised Framework

Aspect	RBI Framework (2017)	Revised Framework (Pilot from 2027)
Primary Focus	Unauthorised electronic transactions	Unauthorised transactions plus social engineering and coercion-based frauds
Nature of Fraud Covered	Mainly technical breaches and hacking	Technical breaches, phishing, impersonation, digital arrest scams and related frauds
Customer Protection	Limited to specified unauthorised transactions	Expanded protection under defined eligibility conditions
Reporting Mechanism	Bank reporting procedures	Reporting through 1930 within prescribed timeline
Post-Reporting Liability	Limited protection	Zero liability for subsequent fraudulent transactions after timely reporting

The revised framework represents a significant evolution in India's digital banking regulation. Instead of focusing solely on technical unauthorised transactions, it explicitly recognises social engineering and coercion-based frauds as major threats to the digital economy, thereby aligning consumer protection with the changing nature of cybercrime.

Conclusion

The RBI's revised compensation framework reflects the reality that the weakest link in cyber security is often human behaviour rather than technology alone. By extending protection to victims of social engineering and coercion-based frauds, the framework strengthens trust in India's digital payment ecosystem and supports the broader objectives of financial inclusion and Digital India. Going forward, sustained public awareness, adaptive regulation, stronger cyber security infrastructure and continuous innovation in fraud detection will be essential for ensuring secure, resilient and inclusive digital finance.

Reader's Note — About This Current Affairs Compilation

Dear Aspirant,

This document is part of the PrepAlpine Current Affairs Series — designed to bring clarity, structure, and precision to your daily UPSC learning.

While every effort has been made to balance depth with brevity, please keep the following in mind:

1. Orientation & Purpose

This compilation is curated primarily from the UPSC Mains perspective — with emphasis on conceptual clarity, analytical depth, and interlinkages across GS papers.

However, the PrepAlpine team is simultaneously developing a dedicated Prelims-focused Current Affairs Series, designed for:

- factual coverage
- data recall
- Prelims-style MCQs
- objective pattern analysis

This Prelims Edition will be released separately as a standalone publication.

2. Content Length

Some sections may feel shorter or longer depending on topic relevance and news density. To fit your personal preference, you may freely resize or summarize sections using any LLM tool (ChatGPT, Gemini, Claude, etc.) at your convenience.

3. Format Flexibility

The formatting combines:

- paragraphs
- lists
- tables
- visual cues

—all optimised for retention.

If you prefer a specific style (lists → paras, paras → tables, etc.), feel free to convert using any free LLM.

4. Monthly Current Affairs Release

The complete Monthly Current Affairs Module will be released soon, optimized to a compact 100–150 pages — comprehensive yet concise, exam-ready, and revision-efficient.

PrepAlpine