CURRENT AFFAIRS: 01.06.2026

Ministry of Corporate Affairs

Azadi Ka Amrit Mahotsav

Insolvency and Bankruptcy Code (IBC) completes 10 years

IBC resolution process has facilitated realisation of over ₹4 lakh crore for creditors

Posted On: 28 MAY 2026 6:35PM by PIB Delhi

Why in News?

The **Insolvency and Bankruptcy Code (IBC), 2016** completed a decade of its implementation. Marking this milestone, the government highlighted the structural transformation of India's corporate resolution framework, which has significantly reduced **Non-Performing Assets (NPAs)** and revived financially distressed businesses.

Summary

- **IBC, 2016 has transformed India's insolvency ecosystem** by enabling ₹4.32 lakh crore recovery, reducing bank NPAs from 11.8% (2017) to 2.1% (2025), promoting credit discipline, and shifting India from a debtor-in-possession to a creditor-in-control model.
- **However, persistent challenges remain**, including judicial delays (average resolution time of 744 days), declining recovery rates, large creditor haircuts, NCLT capacity constraints, and real-estate insolvency complexities, necessitating institutional reforms and faster resolution mechanisms.

What are the Achievements of IBC, 2016?

- **Massive Debt Recovery:** Till March 2026, the resolution process facilitated the realisation of **nearly Rs 4.32 lakh crore for creditors**.
  - The recovery rate stands at an impressive **167% against the liquidation value** of the assets.
- **Drastic Reduction in NPAs:** By fostering strict credit discipline, ending the era of strategic defaults, and helping address **India's twin balance sheet problem** (stressed corporate balance sheets and high bank NPAs), the IBC played a foundational role in reducing the Gross NPA ratio of **Scheduled Commercial Banks** to a 12-year low of 2.1% (as of September 2025), down sharply from a peak of 11.8% in 2017.
  - According to the RBI's Report on Trend and Progress of Banking in India (2024–25), the IBC is the single most effective tool for banks, vastly outperforming legacy mechanisms like **SARFAESI Act (Securitisation and Reconstruction of Financial Assets and Enforcement of Security Interest), 2002.**
- **Focus on Rescue over Liquidation:** A**round 58% companies were successfully rescued**, fulfilling the IBC's primary mandate of reviving businesses rather than merely liquidating them.
- **The "Deterrent Effect":** Over 30,000 cases involving roughly Rs **14 lakh crore were resolved at the pre-admission stage** before reaching the **National Company Law Tribunal (NCLT).**
  - The mere threat of losing control of their companies forced promoters to settle dues outside formal bankruptcy proceedings.

- **Improved Global Standing:** Average resolution timelines have been slashed from 6–8 years to approximately 2 years.
  - Recognizing these systemic efficiencies, **S&P Global Ratings upgraded India's insolvency framework from 'Group C' to 'Group B'**.

What is the Insolvency and Bankruptcy Code (IBC), 2016?

- **About**: The **Insolvency and Bankruptcy Code (IBC), 2016,** is India's overarching legislative framework governing the insolvency and bankruptcy of corporate entities, partnership firms, and individuals.
  - Enacted on the recommendations of the **Bankruptcy Law Reforms Committee (BLRC) (2015)** headed by **T.K. Viswanathan,** the IBC consolidated a fragmented legacy framework (which included the **Sick Industrial Companies (Special Provisions) Act, 1985**, SARFAESI Act 2002, and the Recovery of Debts and Bankruptcy Act, 1993 (RDB Act)) into a single, unified law.
  - IBC introduced a **unified, creditor-driven, and time-bound mechanism to resolve financial distress.**
  - The fundamental paradigm shift introduced by the IBC was moving India from a **"debtor-in-possession"** regime, where promoters retained control of the defaulting company, often stalling recovery, to a **"creditor-in-control"** model.
- **Pillars of the IBC:**

Pillar	Entity	Function
Regulator	Insolvency and Bankruptcy Board of India	Regulates and supervises the insolvency ecosystem, including IPs (Insolvency Professionals), IPAs (Insolvency Professional Agencies), and IUs (Information Utilities); frames and enforces regulations under the IBC.
Adjudicating Authorities (AA)	National Company Law Tribunal and Debt Recovery Tribunal	NCLT handles insolvency cases of companies and LLPs, while DRT deals with individuals and partnership firms.
Professionals	Insolvency Professionals (IPs)	Licensed professionals who manage the affairs of the defaulting entity and conduct the **Corporate Insolvency Resolution Process (CIRP).**
Data Repositories	Information Utilities (IUs)	Centralized repositories (e.g., National e-Governance Services Ltd.) that store financial information and provide authenticated evidence of default, reducing litigation and delays.

Corporate Insolvency Resolution Process (CIRP)

- **Application for Initiation:** Upon a payment default, a Financial Creditor, an Operational Creditor, or the Corporate Debtor itself applies to the NCLT to initiate the CIRP.
- **Admission and Moratorium:** Once admitted, the NCLT declares a "Moratorium," freezing all parallel legal proceedings and debt recovery actions against the company to ensure its assets are not stripped while a resolution is sought.
- **Constitution of the CoC:** An Interim Resolution Professional (IRP) takes over the company's management and forms the **Committee of Creditors (CoC)**, comprising solely of financial creditors.
- **Resolution or Liquidation:** The CoC evaluates resolution plans submitted by prospective buyers.
  - If a plan is approved by a 66% voting share, it is submitted to the NCLT for final clearance. If no plan is approved within the deadline, the NCLT orders the mandatory liquidation of the company.
- **Time Period:** The IBC mandates that the resolution process must be completed within a maximum of **330 days**, including all legal extensions and litigation time.

Amendments to IBC, 2016

- The **IBC (Amendment) Act, 2019,** introduced a **330-day deadline for completing the CIRP**, mandated the NCLT to decide on insolvency applications within **14 days**, and brought **personal guarantors** under the insolvency framework.
- The **IBC Second Amendment Act, 2020,** provided relief during the **Covid-19 pandemic** by **temporarily suspending the initiation of CIRP** against defaulting companies.
- The **IBC (Amendment) Act, 2021,** introduced the **Pre-Packaged Insolvency Resolution Process (PPIRP)**, offering a faster and cost-effective insolvency resolution mechanism for **MSMEs**.
- **IBC (Amendment) Act, 2026:**
  - **Introduces Creditor-Initiated Insolvency Resolution Process (CIIRP)** as an out-of-court mechanism for select financial institutions, enabling faster and more efficient debt resolution.
    - CIIRP can be initiated with the consent of **at least 51% of financial creditors**, enabling faster and more efficient debt resolution.
  - **Strengthens the "Clean Slate Principle"**, ensuring that approved resolution plans extinguish past claims against the corporate debtor unless specifically preserved.
  - **Enhances the role of the Committee of Creditors (CoC)** by granting greater authority in appointing/removing liquidators and overseeing liquidation proceedings.
  - **Clarifies that government dues are not secured creditors**, thereby maintaining priority for secured financial creditors during asset distribution.
  - **Introduces penalties for frivolous filings** and provides clearer definitions for avoidance transactions and fraudulent/wrongful trading.

How safe is India's critical national infrastructure?

Over the last few decades, critical infrastructure and services have been scaled up through automation, the Internet of Things and AI. However, this has also made them more vulnerable to attacks through IoT devices, highlighting the need for a policy framework to safeguard our infrastructure

Why in News?

Concerns regarding the safety of India's **Critical National Infrastructure (CNI)** have come to the forefront, driven by the rapid integration of **Artificial Intelligence (AI), the Internet of Things (IoT), and Operational Technology (OT)** networks.

- While digitalisation has improved efficiency, it has significantly expanded the country's vulnerability to remote cyber-disruptions, making infrastructure security a top-tier national security priority.
- **India's Critical National Infrastructure (CNI)**—including power grids, telecom networks, banking systems, transport networks, and strategic assets—is increasingly vulnerable to cyber threats due to the convergence of IT, OT, and IoT systems, weak IoT security, foreign supply-chain risks, legacy software, and emerging quantum-computing threats.
- **To strengthen CNI security**, India has launched initiatives such as NCIIPC, CERT-In cyber drills, Trusted Telecom Portal, IndiaAI Mission, and STQC hardware verification, while future priorities include adopting Post-Quantum Cryptography (PQC), implementing Zero-Trust Architecture (ZTA), achieving silicon sovereignty, establishing a unified cyber command, and enhancing cybersecurity awareness and talent.

What is Critical National Infrastructure (CNI)?

- **Definition:** CNI refers to the physical and cyber-based systems, assets, and networks that are so vital to the country that their incapacity or destruction would have a debilitating impact on national security, economic stability, public health, or safety.
- **Key Sectors in India:** Under the **Information Technology Act, 2000**, the government established the **National Critical Information Infrastructure Protection Centre (NCIIPC)** to protect these fundamental sectors:
  - **Energy and Power:** Power grids, nuclear plants, and refineries.
  - **Transport:** Railways, airports, shipping corridors, and digital navigation systems.
  - **Banking and Finance:** Payment gateways (like UPI), banking networks, and stock markets.
  - **Telecommunications:** Internet service providers, satellite communications, and 5G networks.
  - **Strategic and Public Enterprises:** Defense networks, centralized public healthcare systems, and urban water distribution telemetries.

Note: Information Technology (IT): Systems that manage, process, store, and transmit digital data and information.

- **Artificial Intelligence (AI):** Technology that enables computers to simulate human intelligence, learning, and decision-making.
- **Internet of Things (IoT):** A network of connected devices that collect and exchange data over the internet.
- **Operational Technology (OT) Networks:** Systems that monitor and control industrial processes and critical infrastructure.

What are the Major Threats and Vulnerabilities Faced by India's CNI?

- **The IT-OT-IoT Triad:** Modern infrastructure relies on the convergence of Information Technology (IT) (data), Operational Technology (OT) (industrial machinery/SCADA systems), and the Internet of Things (IoT) (sensors).
  - This interconnectedness increases efficiency but significantly expands the attack surface.
  - Historically, OT networks which control physical machinery like power grids and dams were "air-gapped" (isolated from the internet).
  - Connecting these systems to IT and IoT networks for remote monitoring creates a massive attack surface, allowing **hackers to breach an IT server and directly manipulate heavy physical machinery.**
- **Supply Chain Infiltration (Foreign Components):** Loose tender specifications and lower-level procurement processes often allow re-branded or mislabeled foreign equipment to enter sensitive networks.
  - For example, imported IoT sensors, surveillance cameras, or GPS-enabled locks with fraudulent labels can carry hidden malware or allow foreign remote shut-offs of supply routes.
  - For instance, cost-prioritized procurement processes enabled the integration of 1.4 lakh Chinese-made Hikvision surveillance cameras into **Delhi's municipal infrastructure,** creating significant security vulnerabilities.
- **Weak Credentials:** Millions of connected IoT devices lack strong security protocols.
  - Indian infrastructure, such as government mail servers and water quality management software, operates on default manufacturer passwords or hard-coded credentials, making them highly susceptible to unauthorized access and manipulation.
- **The "Quantum" Threat ("Harvest Now, Decrypt Later"):** Critical sectors rely heavily on public-key **cryptography,** which future quantum computers will be able to easily break.
  - This creates a "harvest now, decrypt later" risk, where adversaries may steal encrypted sensitive data today and decrypt it in the future once quantum capabilities mature.
- **Interconnectivity and Cascading Failures:** Modern infrastructure is hyper-connected.
  - A successful cyberattack on a foundational sector like telecommunications can trigger a domino effect, simultaneously crippling banking systems, power distribution, and logistics networks.
- **Legacy Systems and Weak Compliance:** Nearly 60% of Public Sector Undertakings (PSUs) and municipal utilities continue to operate on outdated legacy software.
  - Furthermore, many rely on basic, outdated checklist audits for compliance rather than conducting rigorous, firmware-level security checks or adopting **"Zero-Trust" architectures.**

India's Initiatives to Protect CNI

- **National Critical Information Infrastructure Protection Centre (NCIIPC):** It is the designated national nodal agency for safeguarding Critical Information Infrastructure (CII) in India.
  - Established under the Information Technology (IT) Act, 2000, its primary responsibilities include identifying critical sectors, monitoring cyber threats, and issuing binding security guidelines. The NCIIPC operates as a specialized unit under the **National Technical Research Organisation (NTRO).**
- **Proactive CERT-In Drills:** In 2025, the **Indian Computer Emergency Response Team (CERT-In)** conducted advanced cybersecurity drills, simulating multi-vector attacks across public and private organizations.
  - CERT-In has prepared a **Cyber Crisis Management Plan** to counter cyber attacks and cyber terrorism, implemented by ministries, departments, states and critical sectors
- **I4C (Indian Cybercrime Coordination Centre):** Operating under the Ministry of Home Affairs, **I4C** coordinates the law enforcement response to digital financial fraud and manages the National Cyber Crime Reporting Portal.
- **IT Amendment Rules, 2026:** Introduced an aggressive 3-hour takedown window for **"Synthetically Generated Information" (Deepfakes)** to curb cognitive warfare and AI-generated misinformation targeting public trust.

- **Trusted Telecom Portal:** Mandates that telecom service providers procure 5G and network equipment exclusively from verified "Trusted Sources" to prevent foreign malware from embedding into national networks.
- **IndiaAI Mission:** In early 2026, the government successfully onboarded 38,000 GPUs to power indigenous AI models, decoupling critical national security operations from untrusted foreign cloud infrastructure.
- **STQC Hardware Verification:** The **Standardization Testing and Quality Certification (STQC) directorate** has launched specialized hardware testing to examine imported IoT devices for hidden data-sharing mechanisms.

Revision MCQ Practice (May Month)

1. Consider the following statements regarding International Labour Day:

1. International Labour Day is celebrated every year on 1st May to honour workers' contributions.
2. It originated from the Russian Revolution of 1917.
3. The demand for an eight-hour workday was a key factor behind its origin.
4. The United States celebrates Labour Day in May.

Which of the statements given above are correct?

(a) 1 and 3 only
(b) 1, 2 and 4 only
(c) 2 and 4 only
(d) 1, 3 and 4 only

2. Consider the following statements regarding labour rights in India:

1. Articles 23 and 24 of the Constitution prohibit forced labour and child labour.
2. India has ratified all ILO conventions related to labour rights.
3. Equal pay for equal work is promoted under Article 39.
4. Around 90% of India's workforce is employed in the informal sector.

Which of the statements given above are correct?

(a) 1, 3 and 4 only
(b) 1 and 2 only
(c) 2, 3 and 4 only
(d) 1, 2, 3 and 4

3. Consider the following statements regarding Sikkim's integration with India:

1. Sikkim became a protectorate of India after independence under a treaty signed in 1950.
2. The 35th Constitutional Amendment gave Sikkim full statehood.
3. Article 371F provides special protections to Sikkim.
4. Sikkim became the 22nd state of India in 1975.

Which of the statements given above are correct?

(a) 1, 3 and 4 only
(b) 1 and 2 only
(c) 2, 3 and 4 only
(d) 1, 2, 3 and 4

4. Consider the following statements regarding the Panchayat Advancement Index (PAI):

1. PAI is a global framework launched by the United Nations.
2. It measures the performance of Gram Panchayats using objective indicators.
3. Panchayats are graded from A+ to D based on their performance.
4. Kerala has the highest percentage of 'Front Runner' Panchayats.

Which of the statements given above are correct?

(a) 2 and 3 only
(b) 1, 2 and 4 only
(c) 2, 3 and 4 only
(d) 1 and 4 only

Q. No.	Answer	Explanation
1	**(a)**	Statement 1 is correct (Labour Day is celebrated on 1 May). Statement 3 is correct (8-hour workday demand led to the Haymarket Movement). Statements 2 and 4 are incorrect.
2	**(a)**	Articles 23 and 24 prohibit forced labour and child labour. Article 39(d) promotes equal pay for equal work. About 90% of India's workforce is in the informal sector. India has not ratified all ILO conventions.
3	**(a)**	Sikkim became an Indian protectorate under the 1950 treaty. Article 371F provides special provisions. Sikkim became India's 22nd state in 1975. The 35th Amendment granted Associate State status, not full statehood.
4	**(c)**	PAI is an initiative of the Ministry of Panchayati Raj, not the UN. It evaluates Gram Panchayats through objective indicators, grades them from A+ to D, and Kerala has the highest share of Front Runner Panchayats.