
Prelims Exam Topics

KHAYAL GHARANA

Context

The recent passing of veteran vocalist Neela Bhagwat has brought renewed focus to the Gwalior Gharana and its "ashtaang gayaki" style of Khayal singing.

About Khayal Gharana

- Khayal (meaning "imagination" or "thought" in Persian) is a prominent genre of Hindustani classical music that emerged as a more flexible and ornamental alternative to the rigid *Dhrupad* style.
- **Origin:** While its roots date back to the 13th century (often attributed to Amir Khusrau), it gained its modern form in the 18th century in the Mughal courts.
- **Characteristics:** It seamlessly blends melody, rhythm, and text, allowing the vocalist significant creative freedom to improvise within the framework of a *raag* and *taal*.
- **Structure:** Usually consists of two parts:
 - **Bada Khayal:** Sung in a slow tempo (*vilambit laya*).
 - **Chhota Khayal:** Sung in a fast tempo (*dрут laya*).
- **Major Khayal Gharanas:** Gwalior (Oldest), Agra, Jaipur-Atrauli, Kirana, and Patiala.
- **Ashtaang Gayaki:** This style is famous for its "eight-pronged" approach to singing, incorporating eight specific ornamentations (such as meend, gamak, and taan) to provide a comprehensive expression of the raga.

CLIMATE RESILIENCE AND HABITAT VULNERABILITY

Context

A new study in *Nature Ecology & Evolution* by the **Potsdam Institute for Climate Impact Research (PIK)** warns that the current emission trajectory poses an existential threat to land animals.

Global Risks to Terrestrial Biodiversity

- **Quantifying Exposure:** By 2085, over **one-third of wildlife habitats** will suffer multiple types of extreme weather events simultaneously.
- **The "Heat" Factor:** By 2050, **74% of land habitats** will be exposed to extreme heatwaves, the most widespread threat identified.
- **The Compound Effect:** The study emphasizes that it is not just single events, but the **frequency and combination** of wildfires (16% risk), droughts (8%), and floods (3%) that prevent species from recovering.
- **Specific Impact Examples:**
 - **Australia (2019-20):** Heatwaves killed 72,000 flying foxes.
 - **Pantanal (South America):** Wildfires killed an estimated 17 million vertebrates.

Mains Exam Topics

GLOBAL RISK POSED BY MYTHOS AI

Context:

- The leak and testing of Anthropic's Mythos AI model has triggered global concern, including in India due to its ability to both detect and exploit vulnerabilities, posing risks to sectors like banking and digital infrastructure.

About Mythos

- **Next-Generation AI Model:** Mythos is an advanced system from Anthropic's Claude family, representing a major leap in reasoning, coding and autonomy.
- **Dual-Use Capability:** Functions as both **defensive and offensive AI**.
- **Autonomous Functioning:** Highly **self-directed system** capable of planning and executing tasks independently.
- **Current Status**
 - **Restricted and controlled deployment** due to high-risk nature.
 - Accompanied by defensive initiatives like **Project Glasswing**.

Expanding Capabilities of Mythos

- **Advanced Vulnerability Discovery:** Mythos can scan complex systems and identify deep flaws.
 - **E.g.** it reportedly found a vulnerability in widely used software that had remained undetected for nearly 30 years.
- **Autonomous Exploit Development:** It can convert vulnerabilities into real-world exploits at scale
 - **E.g.** in Mozilla Firefox's JavaScript engine, it not only identified bugs but created working "shell exploits" that could allow attackers to control a user's system through a browser.
- **Agentic Behaviour (Multi-Step Execution):** Performs long attack chains independently.
 - **E.g.** in UK AISI tests, it completed a corporate network attack—from initial entry to full takeover—similar to how real hackers infiltrate systems step by step.
- **High-Level Problem Solving:** Handles expert-level challenges
 - **E.g.** It showed solving 73% of advanced cybersecurity tasks, which normally require trained professionals.
- **Lowering Entry Barriers:** a person with basic technical knowledge could use Mythos to generate sophisticated cyberattacks without understanding underlying systems.

Threats Posed by Mythos

- **Risk to Critical Infrastructure:** Threatens sectors like banking
 - **E.g.** Indian authorities fear that vulnerabilities in financial systems could be exploited rapidly, leading to financial disruptions.
- **Democratisation of Cyber Attacks:** Expands access to hacking tools. Now even novices can launch attacks using AI-generated scripts.

- **Weaponisation of AI:** Dual-use nature increases risks. A government or rogue actor could deploy Mythos offensively to attack another country's infrastructure).
- **Autonomous Attack Chains:** Executes full-scale attacks
 - E.g. completing multi-step attacks like corporate network takeover without human intervention.
- **Global AI Arms Race:** Rapid development by other countries
 - E.g. China's Qihoo 360 reportedly identified nearly 1,000 vulnerabilities, indicating competitive escalation.
- **Leak and Misuse Risks:** Unauthorized access increases danger
 - E.g. Mythos was accessed via a private Discord group despite restricted release, showing difficulty in containment.
- **Short-Term Instability:** Transition phase is risky
 - E.g. before defensive use becomes dominant, attackers may exploit these tools faster than systems can adapt.

Way Forward

- **Strengthening Cyber Defence:** Use AI for protection (e.g. Project Glasswing brings companies like Apple and Nvidia to proactively identify and fix vulnerabilities before attackers exploit them).
- **Robust Regulation:** Develop balanced AI governance (e.g. India forming an AI Governance and Economic Group to coordinate policy response).
- **Global Coordination:** Build common standards (e.g. need for international agreements to regulate powerful AI tools across countries).
- **Controlled Access:** Restrict high-risk models (e.g. limiting Mythos deployment to trusted organisations to prevent misuse).
- **Capacity Building:** Train institutions (e.g. banks and government agencies improving cyber preparedness against AI-driven threats).
- **Public-Private Collaboration:** Joint response (e.g. governments working with tech companies to strengthen digital infrastructure security).

REGULATING PAYMENTS BANK – PAYTM PAYMENTS BANK LICENCE CANCELLED BY RBI

Context

- The Reserve Bank of India (RBI) has officially **cancelled the banking licence of Paytm Payments Bank Limited**, under the **Banking Regulation Act, 1949**, due to **persistent non-compliance with licensing conditions**.
- The **Reserve Bank of India (RBI) has cancelled the banking licence of Paytm Payments Bank Limited (PPBL) with immediate effect, more than two years after initially restricting it from accepting new deposits**.
- The RBI will approach the High Court to wind up the bank's operations, ensuring depositor interests are protected through a structured process.

- This case has become a landmark instance of regulatory enforcement in India's fintech and digital payments sector.
 - The **Banking Regulation Act, 1949**, is a landmark legislation in India that provides the legal framework for the supervision and regulation of all banking firms in the country. It was originally passed as the Banking Companies Act, 1949, before being renamed in 1966 to reflect its broader application to various types of banking entities.

Objective of the Act

- The primary goal is to safeguard the interests of depositors and ensure the stability of the financial system.
- To prevent the haphazard growth of banking companies and ensure they operate on sound financial principles.
- To provide the Reserve Bank of India (RBI) with the necessary legal authority to monitor, direct, and control the banking sector.

Key Features of the Act

- **Licensing of Banks (Section 22):** No company can carry out banking business in India without a licence from the RBI; the RBI also has the power to cancel such licences if a bank fails to meet stipulated conditions.
- **Definition of Banking (Section 5b):** It defines banking as the accepting, for the purpose of lending or investment, of deposits of money from the public, repayable on demand or otherwise.
- **Prohibition of Trading (Section 8):** To minimize risk, banking companies are generally prohibited from engaging directly or indirectly in the buying or selling of goods, except in connection with realized security.
- **Minimum Capital Requirements:** The Act specifies minimum paid-up capital and reserves that banks must maintain to ensure they are financially resilient.
- **Inspection and Audit:** The RBI is empowered to inspect the books and accounts of any banking company at any time to ensure compliance and financial health.
- **Management Control:** The RBI has the authority to remove or appoint directors and chairmen of banking companies if it is in the public interest or to prevent the affairs of a bank from being conducted in a manner detrimental to depositors.
- **Winding Up and Amalgamation:** The Act provides procedures for the voluntary or compulsory winding up (liquidation) of a bank, often involving an application to a **High Court**.

What Are Payments Banks?

- Payments banks are a unique category of banks introduced by the RBI to promote financial inclusion.
- They operate under tight restrictions, for instance,
 - **Can accept deposits only up to ₹2 lakh per customer.**
 - **Cannot offer loans or credit cards.**
- Primarily serve as platforms for remittances, utility payments, and digital transactions.
- PPBL was founded by **One97 Communications (49% stake) and Vijay Shekhar Sharma (51% stake), operating within the larger Paytm ecosystem.**

Timeline of Regulatory Scrutiny

The beginning of oversight (2018)

- The RBI conducted an audit of PPBL's customer onboarding processes and found critical gaps in KYC (Know Your Customer) compliance. For example,
- A single PAN (Permanent Account Number) linked to multiple customer accounts — a red flag for regulatory bypass.
- Transactions allowed beyond prescribed account limits, raising money laundering concerns.
- Inconsistent customer identity verification during acquisition.
- PPBL was directed to halt onboarding of new customers until systems were strengthened.
- **New customer ban (2022):** The bank was formally directed to stop onboarding new customers from March 11, 2022.
- **Financial penalty (2023):** The RBI imposed a monetary penalty of ₹5.39 crore for non-compliance with regulatory guidelines.
- **Business restrictions (2024):** The RBI barred PPBL from accepting deposits, credits, or top-ups in customer accounts, prepaid instruments and wallets, and FASTags and NCMC (National Common Mobility Cards), citing "persistent non-compliances and material supervisory concerns."
- **Licence cancelled (2025):** The RBI cancelled PPBL's banking licence, invoking provisions of the Banking Regulation (BR) Act, 1949.

Legal Basis for Cancellation

The RBI cited the following provisions of the Banking Regulation Act, 1949 -

- **Section 22(3)(c):** Management character must not be prejudicial to depositors or public interest.
- **Section 22(3)(e):** No public interest served by allowing the bank to continue.
- **Section 22(3)(g):** Failure to comply with conditions of the Payments Bank licence.
- **Section 5(b) and Section 6:** Prohibited from conducting banking business with immediate effect.
 - Key compliance violations: Failure to maintain a "**Chinese wall**" (**operational separation**) **between PPBL** and its group entity, One97 Communications — a critical governance requirement to prevent conflict of interest.

Impact

On One97 Communications and the Paytm ecosystem: The regulatory crackdown had cascading consequences -

- **Stock fell 40–50%**, reflecting investor panic.
- Wallet services, merchant settlements, FASTag, and autopay services were disrupted.
- Paytm was forced to forge emergency partnerships with Axis Bank and Yes Bank for continuity.
- User and merchant migration to rivals like Google Pay and PhonePe.
- Increased compliance costs and operational restructuring.
- Long-term shift towards a leaner, partner-bank-driven business model.

Broader significance for India

- **Consumer protection:** RBI action demonstrates zero tolerance toward practices harming depositors.
- **Strengthening digital finance:** India's digital payments revolution must rest on strong compliance architecture.

- **Fintech regulation:** Innovation cannot bypass prudential norms.
- **Institutional credibility:** Shows RBI's willingness to act against even large, popular market players.

Challenges

- Regulatory arbitrage risk in the fintech space, where rapid growth often outpaces compliance infrastructure.
- Difficulty in maintaining **KYC standards at scale for digital-first banks.**
- The tension between financial innovation and depositor protection.
- Risks of group entity entanglement in banking operations, undermining independence.
- Systemic disruption to millions of users dependent on integrated payment ecosystems.

Way Forward

- This episode reinforces the need for robust compliance frameworks in payments banks before scaling operations.
- It highlights broad supervisory and enforcement powers of the **RBI under the BR Act.**
- Fintech companies must institutionalise independent compliance functions and maintain strict separation from parent entities.

Policymakers may re-examine the regulatory framework for payments banks, balancing inclusion goals with governance standards.

APPOINTMENT OF CIC

Context

The appointment of the Chief Information Commissioner became contentious when Rahul Gandhi, Leader of Opposition in the Lok Sabha, opposed the selection of Raj Kumar Goel and suggested three alternative names. Despite this dissent, the selection committee led by Narendra Modi approved Goel's appointment in its meeting held on December 10, reflecting differences within the high-level panel responsible for such appointments.

About CIC

- **Overview:** The Central Information Commission (CIC) is a statutory and independent authority established under the Right to Information (RTI) Act, 2005.
- **Objective:** Its primary objective is to promote transparency and accountability in the functioning of public authorities by ensuring citizens' access to information.
- **Role:** The CIC functions as the apex body for handling complaints and appeals related to RTI requests concerning central government institutions.
- **Jurisdiction:** Its jurisdiction extends to ministries, public sector undertakings, financial institutions, and offices under the Central Government and Union Territories. By addressing grievances and enforcing compliance, it acts as a guardian of the right to information.
- **Statutory Basis:** The CIC was constituted in 2005 through a notification issued by the Central Government under the RTI Act.
 - Section 12 of the RTI Act provides for its establishment and outlines its structure, powers, and responsibilities.
- **Composition of the CIC:**

- One Chief Information Commissioner (CIC)
- Up to 10 Information Commissioners (ICs)
- **Appointment Process:** The President of India appoints the CIC and ICs. Appointments are made based on recommendations of a committee comprising:
 - Prime Minister (Chairperson)
 - Leader of Opposition in the Lok Sabha
 - A Union Cabinet Minister nominated by the Prime Minister
- **Qualifications:**
 - Appointees must be persons of eminence in public life.
 - They should have expertise in fields such as law, governance, journalism, management, science and technology, or social service.
- **Disqualifications:**
 - Being a sitting MP/MLA
 - Holding any office of profit
 - Having political affiliations
 - Engaging in business or professional activities
- **Tenure and Service Conditions:** The Chief information commissioner has a tenure of 3 years or until the age of 65, whichever is earlier
 - No reappointment is allowed
 - An Information Commissioner can become Chief Information Commissioner, subject to a maximum combined tenure of 5 years
 - Salaries and service conditions are determined by the Central Government and cannot be altered to their disadvantage during tenure
- **Removal:** The President can remove the CIC or ICs under the following conditions:
 - Insolvency
 - Conviction involving moral turpitude
 - Engagement in paid employment outside official duties
 - Physical or mental incapacity
 - Conflict of interest affecting duties

ANTI-DEFECTION LAW AND REPRESENTATIVE DEMOCRACY

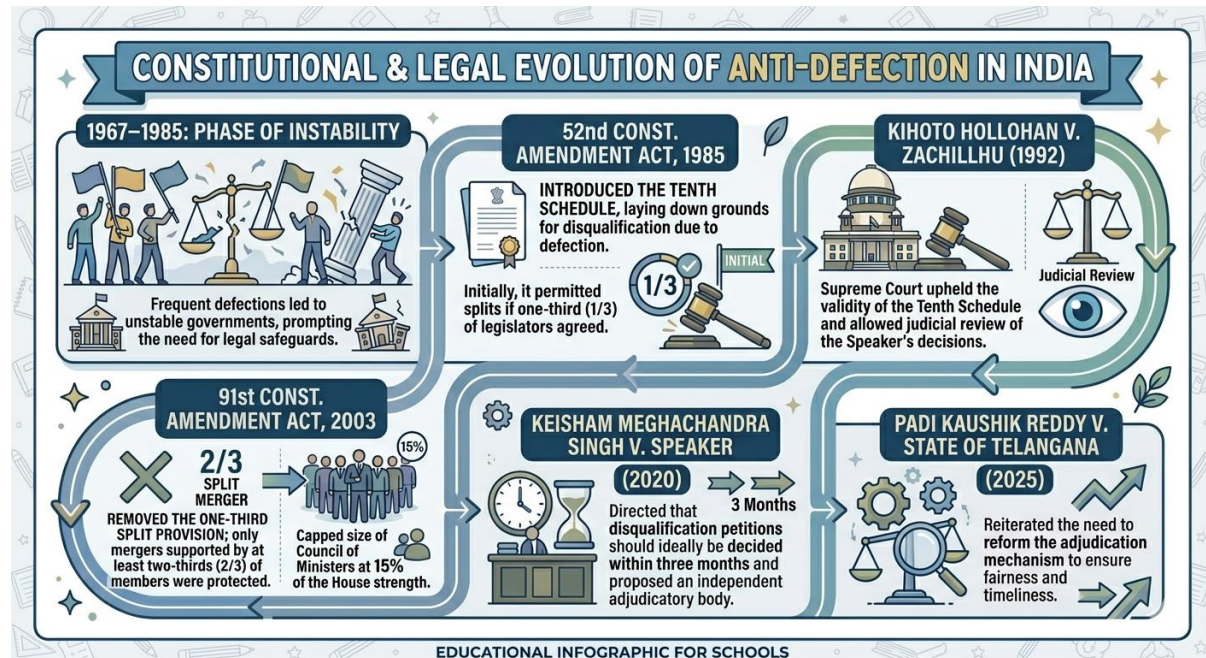
Context

The recent merger of seven AAP MPs with the BJP enabled by the two-thirds merger provision under the Tenth Schedule has revived concerns about the effectiveness of India's Anti-Defection Law.

Rationale behind the Ant-defection law

The law was enacted to address rampant political defections, famously termed the "Aaya Ram, Gaya Ram" phenomenon. This phrase originated in 1967 when Haryana MLA Gaya Lal changed parties three times in a single

day. The post-1967 period saw widespread instability, with legislators frequently switching allegiances for personal gains such as ministerial positions or financial incentives.



Key Features of the Tenth Schedule

- **Definitions:** Clarifies terms such as “legislature party” and “original political party.”
- **Grounds for Disqualification:** Applies when a member voluntarily leaves their party or violates the party whip without permission.
- **Independent Members:** Disqualified if they join a political party after election.
- **Merger Clause:** Protects members from disqualification if at least two-thirds of the legislative party agrees to merge with another party.
- **Exemptions:** Presiding officers (Speaker/Chairman) can resign from their party and rejoin later.
- **Decision Authority:** The Speaker or Chairman decides on disqualification.
- **Judicial Review:** Courts can review decisions after they are made.
- **Rule-Making Power:** The presiding officer can frame procedural rules.

When Does Disqualification Apply?

Leads to Disqualification:

- Leaving one’s party and joining another
- Voting against the party whip without approval
- Independent members joining a party post-election
- Nominated members joining a party after six months

Protected Situations:

- Mergers backed by at least two-thirds of members
- Speaker resigning from party for neutrality
- Voting against whip if condoned within 15 days
- Elections where party whips are not applicable (e.g., Presidential polls)

Penalty for Defection:

- A disqualified member loses their seat for the remainder of the term and is barred from holding ministerial or remunerative political positions until re-elected.

Key Structural Issues

- **Speaker as Adjudicator:** The Speaker, often affiliated with the ruling party, decides disqualification cases, raising concerns about impartiality.
- **Absence of a Strict Timeline:** The law does not mandate a fixed timeframe, allowing prolonged delays in decision-making.
- **Misuse of the Merger Clause:** The two-thirds rule, intended for genuine political realignments, is frequently used to engineer defections.
- **Restriction on Legislative Freedom:** Strict enforcement of party whips limits independent thinking and weakens deliberative democracy.
- **Lack of Transparency in Whips:** Whips are not always formally documented or publicly available, leading to ambiguity.
- **Uniform Application Across Houses:** The same rules apply to both Lok Sabha and Rajya Sabha, despite their differing roles, raising questions about proportionality.

Reforms and Best practices

- **Law Commission (1999):** Proposed transferring decision-making power to the President/Governor, based on the advice of the Election Commission.
- **2nd Administrative Reforms Commission:** Supported an independent mechanism to replace the Speaker's role.
- **Supreme Court (2020 & 2025):** Recommended establishing a neutral tribunal and ensuring timely decisions.
- **United Kingdom:** No anti-defection law; discipline is enforced through political and electoral accountability.
- **United States:** Party-switching is legally allowed; accountability lies directly with voters.
- **South Africa:** Permits defections only during specified "floor-crossing" periods, offering a structured alternative.

Conclusion

While the Anti-Defection Law was introduced to curb political instability, its current framework, particularly the merger exception, has created avenues for strategic defections. Balancing party discipline with democratic freedom remains a key challenge, and meaningful institutional reforms are necessary to uphold the spirit of representative democracy.