GRADIENT IAS

DAILY MAINS QUESTION & ANSWER

This PDF compiles sample question and model answers for UPSC / APSC Mains

Date of publication – 27th November 2023

We have a lot more to offer.
Stay connected with us for free quizzes, notes, newspaper analysis, discussions etc.

Telegram: https://t.me/gradientUPSCAPSC

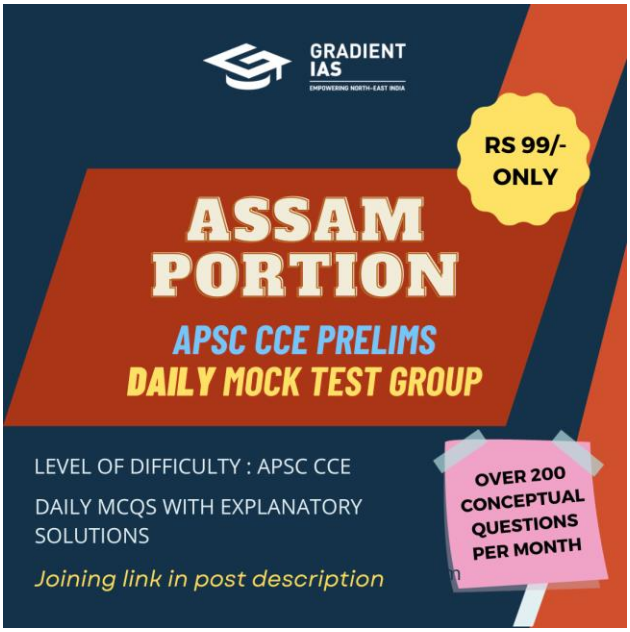
Whatsapp: https://chat.whatsapp.com/DEMKA2G9cpb2gfD5Wr0LhE

Instagram: https://www.instagram.com/gradientias

Facebook: https://www.facebook.com/gradientias

Website: www.gradientias.com

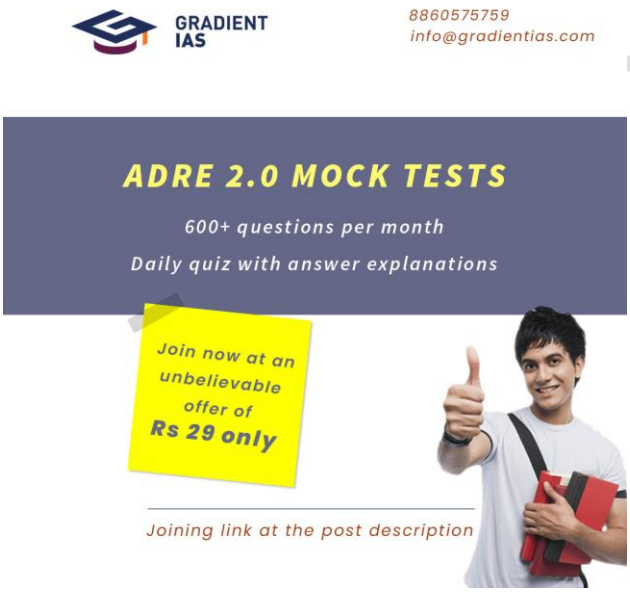
Gradient IAS | H/No - 1A, 2nd Floor
Zoo Road Tiniali, Hridoy Ranjan Path,
Next to Central Bank (Opposite Decora Tent House)
Guwahati – 781024 , 8860575759 / info@gradientias.com



ASSAM MOCK TEST FOR APSC CCE

Daily Online quiz with explanations

Join here - **https://rpy.club/g/9O9WJlrfUR**



ADRE 2.0 MOCK TEST

Daily Online quiz with explanations

Join here - **https://bit.ly/48E99WH**

Q1. Discuss the factors that led to the growth of communalism in India. What efforts must be taken to address the communalism problem in India?

GS I

Communalism related issues

• The concept of communalism is founded on the belief that the most important distinction is religious distinction, which trumps all other distinctions. It is a political ideology that makes use of religious and cultural differences to achieve political objectives. It is the result of contemporary Indian politics, which originated with the British Empire. Communialism has been a major source of tension and violence between religious groups in India.

•The following elements aided the development of communalism in India:

• The British Divide and Rule Policy: During the pre-independence period, the British used the Divide and Rule policy to repress nationalist aspirations. By promoting one community over the other in terms of services and opportunities, Britishers aimed to split Hindus and Muslims. It sowed discord between the two factions. The British used the Partition of Bengal, the establishment of the Muslim League, the Morley-Minto reforms of 1909, and other strategies to separate and dominate.

• The Hindu and Muslim revivalist movements of the nineteenth century were focused with eradicating harmful practises and reforming one's own faith. However, revivalist groups such as the Shuddhi movement of the Arya Samaj and the Wahhabi movement attempted to claim that one religion was superior to another.

• Methods and means of nationalists: Indian nationalists such as Bal Gangadhar Tilak used festivals such as the Ganpati festival and Shivaji Jayanti to mobilise the masses. Such practises, however, had a Hinduistic taste to them that did not relate to other communities.

• A communal and erroneous view of Indian history, particularly during the ancient and mediaeval times, was also critical to its spread. In this regard, British historian James Mill pioneered in the early nineteenth century by designating the ancient period of Indian history as the Hindu period and the mediaeval period as the Muslim period.

• Temperament of Partition: The country's religious partition and the riots, deaths, and rapes that followed were awful, and communalism was at its peak at the time.

Gradient IAS | H/No - 1A, 2nd Floor
Zoo Road Tiniali, Hridoy Ranjan Path,
Next to Central Bank (Opposite Decora Tent House)
Guwahati – 781024 , 8860575759 / info@gradientias.com

• Vote bank politics: After independence, political parties employed appeasement techniques to satisfy diverse ethnic, religious, and cultural groups in exchange for votes. Appeasement methods such as providing amenities and opportunities to certain parts of the population at the expense of others strongly affected this vote bank politics. This has encouraged communalism even more in India.

• The following are measures to address India's communalism problem:

• Value-oriented education: Emphasising ideals like as secularism, humanism, peace, nonviolence, and cultivating a scientific temperament can serve to deter community attitudes.

• Reducing socioeconomic disparities: Poverty and the resulting socioeconomic inequalities are major causes to communal violence. Poverty alleviation programmes, addressing the issue of unemployment, and reducing the socioeconomic backwardness of minorities can all help to alleviate ethnic tensions.

• Using civil society to assist: The government can employ civil society and non-governmental organisations (NGOs) to run activities that promote communal awareness, develop community bonds, and implant communal togetherness principles in the next generation.

• Reforming administration: Codified administrative rules, specialised training for police officers to deal with communal riots, and the development of specific investigative and prosecutorial agencies can all help to quell major communal anger.

• Monitoring by the media: The media has the potential to play a key role in minimising misinformation and facilitating healthy conversations and debates about such issues.

• Adopting international practises: The government may learn from Malaysia, which has developed early-warning signs to prevent racial clashes.

• Communalism has been and continues to be one of our country's greatest impediments to democracy. To solve the problem of communalism in India, focused activities focusing on forging unity within the multiethnic fabric, cultural exchange programmes, and encouraging peace and harmony are required.

Gradient IAS | H/No - 1A, 2nd Floor
Zoo Road Tiniali, Hridoy Ranjan Path,
Next to Central Bank (Opposite Decora Tent House)
Guwahati – 781024 , 8860575759 / info@gradientias.com

Q2. Ransomware has emerged as the most prevalent sort of malicious attack. In this context, discuss the concerns highlighted by ransomware attacks on India's critical infrastructure. In India, what precautions are in place to combat cyber security threats?

GS III

Science and Technology

• Ransomware is a type of cyberattack in which malicious software threatens to publish or restrict access to data or a computer system unless the victim pays the attacker a ransom. According to the Computer Emergency Response Team's (CERT-In) India Ransomware Report 2022, ransomware attacks grew by 53%. Critical infrastructure is the new frontier in cybersecurity. Today, transportation, oil and gas, power, healthcare, dams, ports, and other industries are all attractive targets for cyber-attacks.

• Ransomware attacks on India's critical infrastructure have raised the following issues:

• Threats to Healthcare Infrastructure: Healthcare is one of the most vulnerable industries to cyber-attacks. Last year's ransomware attack on AIIMs Delhi, for example, severely affected outpatient and inpatient digital hospital services such as smart lab, billing, report writing, and appointment scheduling. Similarly, attackers based in Hong Kong attempted to infiltrate the Indian Council of Medical Research (ICMR) website.

• Ransomware attacks constitute a national security risk because they can cause extensive economic damage, disrupt essential national security and public safety services, and steal national secrets. A ransomware cyberattack, for example, compromised Goa's Water Resources Department's flood monitoring system. Similarly, the ransomware Petya attacked India's largest container facility, the Jawaharlal Nehru facility (JNPT).

• Ransomware attacks are getting increasingly common: up to 78% of Indian businesses were victims of computer attacks in 2021. Hackers demanded an average ransom of $1.2 million from Indian firms in order to release their data. Because of their reliance on technology and interconnection, almost every individual and organisation is vulnerable to cyberattacks.

• Threats to the financial sector: The Banking, Finance, and Insurance (BFSI) industry is the most profitable for hackers and cybercriminals. Banking, for example, was one of the top three businesses targeted by ransomware in 2021.

Gradient IAS | H/No - 1A, 2nd Floor
Zoo Road Tiniali, Hridoy Ranjan Path,
Next to Central Bank (Opposite Decora Tent House)
Guwahati – 781024 , 8860575759 / info@gradientias.com

Furthermore, the Central Depository Services Limited (CDSL), India's second-largest depository, discovered a malware intrusion on two of its systems.

• The global WannaCry ransomware attack had an impact in India, damaging systems belonging to the Andhra Pradesh police and the West Bengal state utilities.

• To fight cybersecurity threats, the following steps are already in place in India:

• National Cyber Security Policy 2013: The policy aims to assist the development of a safe computer environment, to enable sufficient trust and confidence in electronic transactions, and to direct stakeholder efforts for cyberspace protection.

• The Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre) was formed to detect hazardous applications and provide free removal tools.

• The Cyber Surakshit Bharat Initiative was established to increase awareness about cybercrime and train Chief Information Security Officers (CISOs) and frontline IT personnel from all government ministries in order to provide proper safety measures and combat the growing threat of cyberattacks.

•The National Cyber Coordination Centre (NCCC) was created to generate the situational awareness needed for current and potential cyber security threats. It allows individuals and organisations to share timely information for preventative, preventive, and protective activities.

• The Information Technology Act of 2000 was enacted, among other things, to provide legal recognition for electronic communication, internet trade, and cybercrime. The IT Act incorporates deterrent features to cope with cyber dangers and cyber-attacks.

• The Indian Computer Emergency Response Team (CERT-In) issues periodical alerts and advisories about the most recent cyber threats and countermeasures.

• To protect the country's essential information infrastructure, the National essential Information Infrastructure Protection Centre (NCIIPC) was established.

• As the world becomes increasingly interconnected as a result of technological breakthroughs such as smart and connected devices, the Internet of Things (IoT), 5G, and real-time communications, cyber security dangers such as ransomware will only increase in critical infrastructure industries. This demands not just enhanced user understanding on a local level, but also global collective cyber security mechanisms.

Gradient IAS | H/No - 1A, 2nd Floor
Zoo Road Tiniali, Hridoy Ranjan Path,
Next to Central Bank (Opposite Decora Tent House)
Guwahati – 781024 , 8860575759 / info@gradientias.com

Q 3. What do you mean by fundamental structure doctrine? Explain its evolution and significance in the preservation of India's constitution.

GS II

Constitution related issues

• A 13-judge constitution court found in 1973 in Kesavananda Bharati v. State of Kerala that Article 368 of the constitution did not empower parliament to change the document's essential framework. The precedent-setting ruling became known as the "basic structure" doctrine. According to this judicial doctrine, certain essential parts of the constitution cannot be changed or eliminated by parliamentary amendments. Various components of the basic structure theory have evolved throughout time, and they now serve as the foundation for judicial review of constitutional amendments.

• The evolution of basic structural doctrine can be divided into three stages:

• The first stage begins with Sankari Prasad's decision and ends with I.C. Golaknath's choice:

• In the Shankari Prasad case, the constitutionality of the First Amendment Act of 1951, which curtailed the right to property, was challenged. The court upheld the constitutionality of the first amendment and also concluded that Article 368 allows parliament to rewrite the constitution with no exception that core rights cannot be modified.

• The majority of the judges in the Sajjan Singh case found, using the same logic as in the Shankari Prasad case, that parliament, under Article 368, can change any section of the constitution, including basic rights.

• In Golak Nath vs. State of Punjab, however, the Supreme Court took a different stance, ruling that parliament could not curtail fundamental rights guaranteed by the Constitution. The court decided that Article 368 lacked substantial change power and instead just offers procedures for altering the constitution.

• Second stage- Following the Golakhnath Scenario and the Keshavananda case decision:

Gradient IAS | H/No - 1A, 2nd Floor
Zoo Road Tiniali, Hridoy Ranjan Path,
Next to Central Bank (Opposite Decora Tent House)
Guwahati – 781024 , 8860575759 / info@gradientias.com

• The battle between the judiciary and the legislature took a new turn after the Golakh Nath ruling.

• In response to Golakh Nath's decision, the then-government implemented a number of constitutional modifications. The Constitutional Amendment Acts of the 24th, 25th, and 29th allowed Parliament the power to change or even eliminate any basic right.

• The Supreme Court ruled in the Keshavanada Bharti case that, while parliament has the authority to amend any provision of the constitution, it cannot use this authority to change or destroy its "basic structure."

• The judges described many parts of the constitution's "basic structure" in the decision. It featured the constitution's supremacy, the republican and democratic form of government, the constitution's secular nature, and the separation of powers between the legislature, executive, and judiciary.

• Third stage, following the Keshavanada Bharti case:

• The main evolution of this philosophy began during the emergency period, as evidenced by the Indira Gandhi v. Raj Narain case. The 39th Amendment made it illegal to dispute the election of the President, Vice President, Speaker, and Prime Minister. The court defined independent election administration as a "basic structure" in the Indira Gandhi v. Raj Narain case.

• In the Minerva Mill decision, the Supreme Court made important clarifications on the application of the basic structural concept. Under parliament's limited capacity to change the constitution, two crucial considerations were added: harmony and balance between fundamental rights and directive principles, and judicial scrutiny.

• The importance of basic structure in preserving the constitution:

Gradient IAS | H/No - 1A, 2nd Floor
Zoo Road Tiniali, Hridoy Ranjan Path,
Next to Central Bank (Opposite Decora Tent House)
Guwahati – 781024 , 8860575759 / info@gradientias.com

• Bringing about social change: The theory promotes constitutional change, laying the path for substantial social transformation via peaceful democratic means.

• Helpful in consolidating democracy: True democracies are founded on the sovereignty of the people, not the rulers. The fundamental structure concept has kept Indian democracy from devolving into an authoritarian state.

• Providing checks and balances: The theory of separation of powers is a fundamental component of the basic framework. As a result, a balance has been struck between the obligations of Parliament and the Supreme Court in safeguarding the Indian Constitution's seamless web.

• Since its inception in the 1970s, basic structure has evolved through various supreme court decisions. It is a means of giving energy to the living principles of the 'Rule of Law' and implies that no one is above the Constitution and that the Constitution is supreme.

Q 4. Discuss the importance of the Digital Personal Data Protection Act of 2023. What are the various issues raised by the bill?

GS I

Government Policies and Interventions

• The Digital Personal Data Protection (DPDP) bill is legislation that defines the rights and duties of citizens on the one hand, and the requirements of data fiduciaries to use gathered data properly on the other. The Bill aims to manage and protect the use of personal data by outlining users' rights and duties, as well as enterprises' obligations.

• The Importance of the Digital Personal Data Protection Act of 2023:

• Right to privacy: The DPDP bill is viewed as a significant step towards addressing long-standing data protection concerns.

• Compliance and transparency: The bill calls for the establishment of the Data Protection Board of India, which will investigate noncompliance and levy penalties. The Board's ability to operate as a digital office, processing complaints, allocating cases, and making judgements via techno-legal means, increases efficiency and transparency.

Gradient IAS | H/No - 1A, 2nd Floor
Zoo Road Tiniali, Hridoy Ranjan Path,
Next to Central Bank (Opposite Decora Tent House)
Guwahati – 781024 , 8860575759 / info@gradientias.com

• A balance between preserving users' rights and boosting digital businesses: Among the important business-friendly aspects of the law are the elimination of criminal penalties for noncompliance, the facilitation of foreign data transfers, and so on. The bill also guarantees data principals a full set of rights, providing responsibility to the data governance framework.

• Consent clause: Personal data can only be processed for authorised purposes with the individual's consent. Before obtaining consent, a notification must be made. As a result, the bill establishes precise standards for responsibility and responsible data handling.

• Implementation of this measure will be beneficial to India's trade negotiations, particularly with regions such as the European Union. Strong privacy regulations in India will be in line with international data protection standards such as the General Data Protection Regulation (GDPR), facilitating smoother data transfers and improving trade partnerships with privacy-conscious countries.

• **Among the issues raised by the bill are:**

• Exemptions for the state: The Bill provides many exemptions for the processing of personal data by the state. Certain aspects of the bill may be avoided by the government due to exemptions for reasons such as national security, relations with other governments, and public order. Critics fear that these exemptions could impair privacy protections and limit the law's efficacy.

• May impinge on the right to privacy: In 2017, the Supreme Court ruled that any infringement on the right to privacy must be proportionate to the need for such intervention. The Bill authorises the central government to exclude processing by government agencies from any or all provisions in the interest of achieving goals like as state security and public order. This begs the question of whether or not these exemptions will pass the proportionality test.

• The Bill does not address harm resulting from personal data processing: According to the Srikrishna Committee report from 2018, harm is a conceivable outcome of personal data processing. Material losses such as financial loss and loss of access to benefits or services are examples of harm. Identity theft, loss of reputation, discrimination, and unjustified surveillance and profiling are all possibilities. The DPDP bill

Gradient IAS | H/No - 1A, 2nd Floor
Zoo Road Tiniali, Hridoy Ranjan Path,
Next to Central Bank (Opposite Decora Tent House)
Guwahati – 781024 , 8860575759 / info@gradientias.com

does not address the risks of harm that may arise from data processing.

• There is no right to data portability or the right to be forgotten. The right to data portability allows data principals to receive and transfer their data from data fiduciaries for their own use. It gives the data owner more control over their data. The right to be forgotten refers to an individual's ability to limit the disclosure of personal data on the internet. These rights are founded on autonomy, transparency, and accountability. These, however, are not included in the bill.

• Adequacy of protection in the case of cross-border data transfer: The Bill states that the government may restrict the transmission of personal data to specific countries via notification. This indicates that personal data may be transferred to any other country without restriction. Data held in another nation may be more exposed to breaches or unauthorised sharing with foreign governments and business companies if that country has strong data protection regulations.

• With the growth of the digital economy, user privacy is critical in the digital era. As a result, the Digital Personal Data Protection Bill provides legal support to the Supreme Court's decision in the case of Justice K.S. Puttaswamy (Retd) vs. Union of India. Individuals gain substantial rights under the measure, including increased awareness, decision-making autonomy, and control over their personal data.

Q 5. In the Right to Privacy case, the Supreme Court said that any limitations on privacy must be reasonable. Is it in the best interests of society to conduct widespread surveillance using facial recognition? Examine its application in terms of internal security and the hazards it poses.

GS II

Constitution related issues

• **Introduction:**

• The Supreme Court stated in K.S. Puttaswamy v. Union of India (the "right to privacy case") that the right to privacy is a component of the right to life, which is a basic right, but it can be lowered if the interests of society outweigh the right to personal liberty.

• It used the reasonableness standard from Article 21's reasonable limits to limit this privilege.

• **It is a Triple Test that must satisfy the following criteria:**

• It must be supported by legislation, i.e. a statue.

• There must be a valid state interest.

• Proportionality test: The societal interest must be balanced against the reduced right to privacy.

• To evaluate the lifespan of the facial recognition system, we must apply the Triple Reasonability Test, weighing the benefits and hazards.

• The benefits of using a facial recognition technology for widespread surveillance in society include increased security and labor automation.

• **Enhanced security:**

• It helps law enforcement by making it easier to find criminals, thieves, and other trespassers, among other things.

• Maintaining internal security: Using merely a face scan, facial recognition can help detect terrorists or other offenders.

• Safer technology: It cannot be hacked because there is nothing to steal or change, such as a password.

• Personal surveillance cameras and facial recognition software can be used to secure personal electronics.

• Faster processing: The process of recognizing a face takes a second or less, allowing for quick and efficient verification of a person. Furthermore, this technology is tough to deceive, which is a positive.

• Seamless integration: It is fairly simple to integrate; it does not necessitate the expenditure of additional funds, and most facial recognition solutions are compatible with the majority of security software.

• **Automation of identification:**

• Reduces human errors: Previously, security guards had to perform manual identification of a person, which took too long and was not very accurate; however, 3D facial recognition technology and the use of infrared cameras significantly increased facial recognition accuracy and made it extremely difficult to fool.

• More financially viable: hiring individuals for any purpose is always expensive.

• Identification technique that not only takes seconds but is also very accurate.

• Threats posed by mass surveillance using a facial recognition system:

• Breach of Privacy: When coupled with CCTV systems, the operator can track your exact location at all times, equivalent to digital stalking. The principle of Consent is broken because the technology is automated.

• Civil-Political Misuse: The example of China, which maintains track of its citizens' activities with such activities, demonstrates the potential hazards of such a system.

• It may jeopardize civil liberties and democratic rights.

• It could be used to infiltrate intimate relationships.

• Vulnerability in recognition: Because no software is perfect, even minor changes in camera angle or appearance might inevitably result in an error, posing two problems:

• Problem of False Negative: Such a system is not foolproof, and it is not a replacement for intelligence gathering because it is known to falter more frequently than known.

• False Positive Problem: A system like this can incorrectly identify a case, leading to arbitrary arrests of people who have nothing to do with any crime.

• Data Security: Because misusing previously stored data, such as theft, is conceivable, data security is another issue.

• If such dangers remain, then mass surveillance via facial recognition is unquestionably

Gradient IAS | H/No - 1A, 2nd Floor
Zoo Road Tiniali, Hridoy Ranjan Path,
Next to Central Bank (Opposite Decora Tent House)
Guwahati – 781024 , 8860575759 / info@gradientias.com

a threat to personal liberty since it violates our privacy and threatens civil, democratic, and political rights.

• **However, we may address these problems by implementing:**

• improved regulations,

• Infrastructure for data security that is efficient and

• Improved legal and organizational structures that ensure accountability.

• **Conclusion:**

• Given the economic and security benefits that such technologies provide, if these solutions can address the concerns, this would undoubtedly pass the triple test of reasonableness. Because this technology is now possible, it would be difficult to stop its use indefinitely, so it is in the best interest of society to frame a set of rules and an organizational structure to regulate its inevitable adoption.

Q 6. Discuss the features of the whistleblower protection framework. Also deliberate on is it sufficient to protect the honest from the corrupt in India? Discuss.

GS II

Government Policies and Interventions

• **Introduction:**

• A whistleblower is a public servant or any other person, including an NGO, who discloses information to the CVC or State Vigilance Commission about the corrupt use of public funds or resources.

• **Mechanisms for protecting whistleblowers in India:**

• **2014 Whistleblower Protection Act:**

Gradient IAS | H/No - 1A, 2nd Floor
Zoo Road Tiniali, Hridoy Ranjan Path,
Next to Central Bank (Opposite Decora Tent House)
Guwahati – 781024 , 8860575759 / info@gradientias.com

• It seeks to protect the identity of whistleblowers, defined as individuals who make a public interest disclosure related to an act of corruption, misuse of power, or criminal offense committed by a public servant; the Vigilance Commission shall not disclose the complainant's identity except to the department head if he deems it necessary.

• The CVC Act:

• It provides for the CVC and state VCs to initiate investigations into complaints filed by anyone against any official in the AIS category or Group A officers.

• The Lokpal Act:

• Its mission includes all categories of public officials, including the Prime Minister, Ministers, Members of Parliament, and Group ABCD officers, and it has the authority to oversee and supervise any investigation conducted by the CVC in such a situation; the Lokayukta at the state level has similar powers.

• The Right to Information Act offers whistleblowers enormous influence by requiring officers to divulge specific sorts of information.

• However, such measures are sometimes considered as insufficient:

• Limitations on information sharing: The government may refuse to provide information if it believes it is required for national security/interest or foreign relations, however these are overly broad and subjective categories.

• Other countries' whistleblower laws additionally limit the revelation of certain types of information, including as information relating to national security and intelligence, information obtained in a fiduciary capacity, and any disclosure expressly prohibited by law.

• Lack of physical protection: Since the enactment of the RTI Act, about 100 RTI advocates have been assassinated across the country, and many more are harassed on a daily basis.

• Lack of expedited hearings: When cases of corruption are delayed, the corrupt gain access to authority, weakening the case for justice.

Gradient IAS | H/No - 1A, 2nd Floor
Zoo Road Tiniali, Hridoy Ranjan Path,
Next to Central Bank (Opposite Decora Tent House)
Guwahati – 781024 , 8860575759 / info@gradientias.com

• Investigation via current mechanisms: The CVC and CBI, which are crucial investigating bodies in accusations of corruption, are sometimes dismissed as "caged parrots," creating concerns about their independence and consequently impartiality.

• Conclusion:

• Various legal experts in India, including Retd. CJI Madan B. Lokur, believe that the Whistleblower Protection Act, 2014, should be fully revised to incorporate improved mechanisms to secure whistleblowers' physical safety, fast track courts, and independent investigation.

Q 7. What are crucial minerals? Explain why critical minerals are important for a country's prosperity.

GS I

Geography related issues

• A mineral is labelled as critical when the risk of supply shortage and associated economic impact is relatively higher than for other raw materials; these minerals are critical for a country's economic development and national security, and their lack of availability or concentration of extraction or processing in a few geographical locations could lead to supply chain vulnerabilities and even supply disruption.

• The importance of key minerals for a country's development and advancement includes the following:

• Economic importance: Critical minerals play a role in a variety of economic sectors, including information and communication technology, semiconductors, advanced

Gradient IAS | H/No - 1A, 2nd Floor
Zoo Road Tiniali, Hridoy Ranjan Path,
Next to Central Bank (Opposite Decora Tent House)
Guwahati – 781024 , 8860575759 / info@gradientias.com

manufacturing inputs, and materials such as defence applications, permanent magnets, ceramics, and so on.

• Transition to electric vehicles: The rapid adoption of electric vehicles is increasing demand for critical minerals such as cobalt, nickel, lithium, and rare earth elements.

• Increasing self-reliance: As a result of government initiatives such as Make in India, Smart City, Atmanirbhar Bharat, the 100 GW target for renewable energy, and the Production Linked Incentive (PLI) schemes, India's demand for critical minerals is expected to rise significantly.

• Clean energy technologies: As India strives for indigenous development of emerging technologies in the clean energy sector, scaling up manufacturing operations for components such as solar panels, wind turbines, and so on becomes critical, and critical minerals are important for meeting the "Net Zero" commitment.

• Building supply chains: The discovery of mineral riches and the identification of areas of its potential through the use of new technology is critical for India's competitive value chains.

• National security: Critical minerals are required for defence, aerospace, nuclear, and space applications because they can perform complex functions and withstand extreme temperatures; they are also necessary for ensuring defence preparedness and achieving self-reliance in the defence sector.

• As a result, India's focus on critical minerals stems from the realisation that the next economic growth story must follow two parallel processes: improving living standards and establishing manufacturing in strategic sectors, and following and investing more in sustainable models of growth, energy, and lifestyle by focusing on decarbonization.

Gradient IAS | H/No - 1A, 2nd Floor
Zoo Road Tiniali, Hridoy Ranjan Path,
Next to Central Bank (Opposite Decora Tent House)
Guwahati – 781024 , 8860575759 / info@gradientias.com