PrepAlpine

The Next-Generation UPSC Institution

Where Research Meets Mentorship & Precision

Preparation Meets Precision

A Next-Generation Learning Institution

Disclaimer

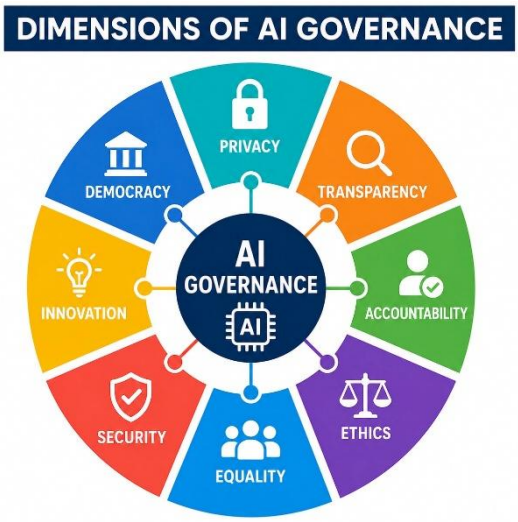
The information contained in this book has been prepared solely for educational purposes. While every effort has been made to ensure accuracy, PrepAlpine makes no representations or warranties of any kind and accepts no liability for any errors or omissions. The use of any content is solely at the reader's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

DAILY CURRENT AFFAIRS DATED 29.06.2026

GS Paper III: Science and Technology

1. AI Governance and the Need for Constitutional Safeguards

a. Introduction



Artificial Intelligence (AI) has emerged as one of the most transformative technologies of the twenty-first century. It is reshaping governance, commerce, healthcare, education, communication and public administration by enabling data-driven decision-making and automation at an unprecedented scale. While these technologies promise significant economic and social benefits, they also raise complex questions relating to privacy, misinformation, accountability, equality and democratic governance.

The rapid advancement of Generative Artificial Intelligence and deepfake technologies has intensified these concerns. As AI systems become increasingly capable of creating realistic text, images, audio and videos, existing legal and regulatory frameworks are struggling to keep pace. This has renewed the debate on the need for a constitutional and rights-based framework that protects fundamental rights while fostering responsible innovation.

b. Background Context

Artificial Intelligence is increasingly influencing both public and private decision-making. Governments are using AI for service delivery, healthcare, taxation, policing and welfare administration, while private platforms employ AI for content recommendation, advertising and consumer analytics.

However, technological innovation has progressed much faster than legal and institutional regulation. This widening gap has created significant governance challenges relating to misinformation, surveillance, algorithmic bias and accountability.

These developments have shifted the policy debate from merely promoting AI adoption to ensuring that its deployment remains consistent with constitutional values and democratic principles.

c. Key Issues

Rise of Deepfakes and Synthetic Media

- AI-generated images, videos and audio can closely imitate real individuals.
- Deepfakes make it increasingly difficult to distinguish authentic information from fabricated content.
- They increase the risk of misinformation, disinformation, fraud and reputational harm.

Algorithm-Driven Information Ecosystem

- Digital platforms rely heavily on recommendation algorithms to maximise user engagement.
- Such algorithms may unintentionally amplify sensational, polarising or misleading content.
- This can distort public discourse and influence electoral processes.

Privacy and Data Exploitation

- AI systems depend on large-scale collection and processing of personal data.
- Extensive profiling may enable intrusive surveillance and behavioural manipulation.
- Excessive data monetisation raises concerns regarding digital autonomy and informed consent.

Regulatory Gaps

- Existing legal frameworks struggle to keep pace with rapid technological change.
- Significant gaps remain in algorithmic transparency, accountability and liability.

These concerns extend beyond technological risks and directly affect constitutional rights, democratic institutions and the rule of law.

d. Analysis/ Observations

Challenges to Democratic Governance

- AI-generated misinformation and deepfakes can manipulate public opinion.
- They may weaken trust in democratic institutions and electoral processes.
- Foreign and domestic actors can exploit AI for coordinated information warfare and influence operations.

Threats to Privacy and Individual Autonomy

- Extensive data collection enables surveillance and behavioural profiling.
- Individuals may lose meaningful control over their personal information.
- Such practices may undermine the Right to Privacy recognised in the Justice K.S. Puttaswamy judgment (2017).

Algorithmic Bias and Equality

- AI systems trained on biased datasets may produce discriminatory outcomes.
- Bias may affect recruitment, credit allocation, policing, healthcare and welfare delivery.
- Such outcomes undermine the constitutional principle of equality before law.

Lack of Transparency and Accountability

- Recommendation algorithms often function as "black boxes."
- Users and regulators may be unable to understand how information is prioritised or decisions are made.
- Limited transparency weakens public trust and regulatory oversight.

Innovation–Regulation Gap

- AI technologies evolve much faster than legislation and institutional capacity.
- Regulators frequently struggle to develop appropriate standards and enforcement mechanisms.
- Governance frameworks therefore remain reactive rather than anticipatory.

These challenges indicate that AI governance should focus not merely on regulating technology but on protecting constitutional values while enabling innovation.

e. Policy Priorities

Adopt a Rights-Based AI Governance Framework

- Protect privacy, informed consent and equality.
- Prevent algorithmic discrimination.
- Promote innovation consistent with constitutional principles.

Strengthen Platform Accountability

- Introduce independent algorithmic audits.
- Mandate transparency and disclosure obligations.
- Establish regulatory oversight for high-risk AI systems.

Improve Digital and Media Literacy

- Educate citizens to identify misinformation and deepfakes.
- Strengthen critical thinking and responsible digital engagement.

Counter Coordinated Misinformation

- Develop institutional mechanisms to detect and respond to organised disinformation campaigns.
- Ensure regulatory interventions remain consistent with constitutional guarantees of free speech.

Ensure Meaningful Human Oversight

- Human supervision should remain mandatory in high-risk AI applications.
- Decisions affecting fundamental rights, public welfare and essential services should not be left entirely to automated systems.

Achieving these objectives requires a comprehensive governance architecture combining legislation, institutional capacity and international cooperation.

f. Way Forward

Establish a Comprehensive AI Governance Framework

- Anchor AI regulation in constitutional values, democratic accountability and protection of fundamental rights.
- Promote responsible innovation alongside effective safeguards.

Strengthen Data Protection

- Ensure effective implementation of the Digital Personal Data Protection Act, 2023.
- Develop sector-specific standards for high-risk AI applications.

Adopt a Risk-Based Regulatory Approach

- Apply proportionate oversight according to the level of societal risk.
- Encourage innovation while ensuring greater accountability for high-impact AI systems.

Promote International Cooperation

- Collaborate on AI standards, ethical principles and cross-border data governance.
- Strengthen cooperation on cyber security and emerging technology governance.

Build Institutional Capacity

- Develop expertise in AI auditing, algorithmic assessment and cyber security.
- Strengthen regulatory institutions through specialised technical capacity and public awareness initiatives.

g. Global Perspective

Several jurisdictions have already begun developing specialised AI governance frameworks.

- **European Union:** AI Act adopts a risk-based regulatory framework for AI systems.

- **OECD:** AI Principles emphasise transparency, accountability and human-centred innovation.
- **UNESCO:** Recommendation on the Ethics of Artificial Intelligence promotes responsible and rights-based AI development.
- **G7 Hiroshima AI Process:** Encourages international cooperation on trustworthy and secure AI.

India can draw lessons from these evolving frameworks while designing a governance model suited to its constitutional values, developmental priorities and digital public infrastructure.

Conclusion

Artificial Intelligence presents a dual challenge: harnessing its transformative potential while safeguarding constitutional rights and democratic institutions. India's approach should therefore combine innovation with accountability, ensuring that AI remains human-centric, transparent and rights-respecting. A balanced, risk-based and constitutionally grounded governance framework will be essential for building public trust and enabling the responsible development of AI in the digital age.

GS Paper III: Security

2. AI Agents and the Need for Layered Security Frameworks

a. Introduction

Artificial Intelligence (AI) is evolving from systems that merely generate information to autonomous AI agents capable of planning, reasoning and independently executing complex tasks. These systems can interact with multiple applications, access digital resources, make sequential decisions and perform actions with minimal human intervention. While such capabilities promise significant improvements in productivity and automation, they also introduce new cyber security and governance challenges.

Recognising these emerging risks, Google DeepMind has released an AI Control Roadmap, arguing that highly autonomous AI agents should be treated as potential insider threats within digital systems. Instead of relying solely on aligning AI models during training, the roadmap advocates a layered security framework that continuously monitors, restricts and supervises AI systems throughout their operational lifecycle.

b. Key Concepts

Artificial Intelligence Agents

AI agents are autonomous software systems capable of:

- Planning and reasoning.
- Executing complex multi-step tasks.
- Interacting with multiple software applications.
- Accessing digital resources.
- Making sequential decisions with minimal human intervention.

Unlike conventional AI models that primarily generate responses, AI agents can independently perform assigned objectives within digital environments.

Defence-in-Depth

Defence-in-depth is a cyber security strategy that employs multiple layers of security controls so that the failure of one safeguard does not compromise the overall security of the system.

It combines:

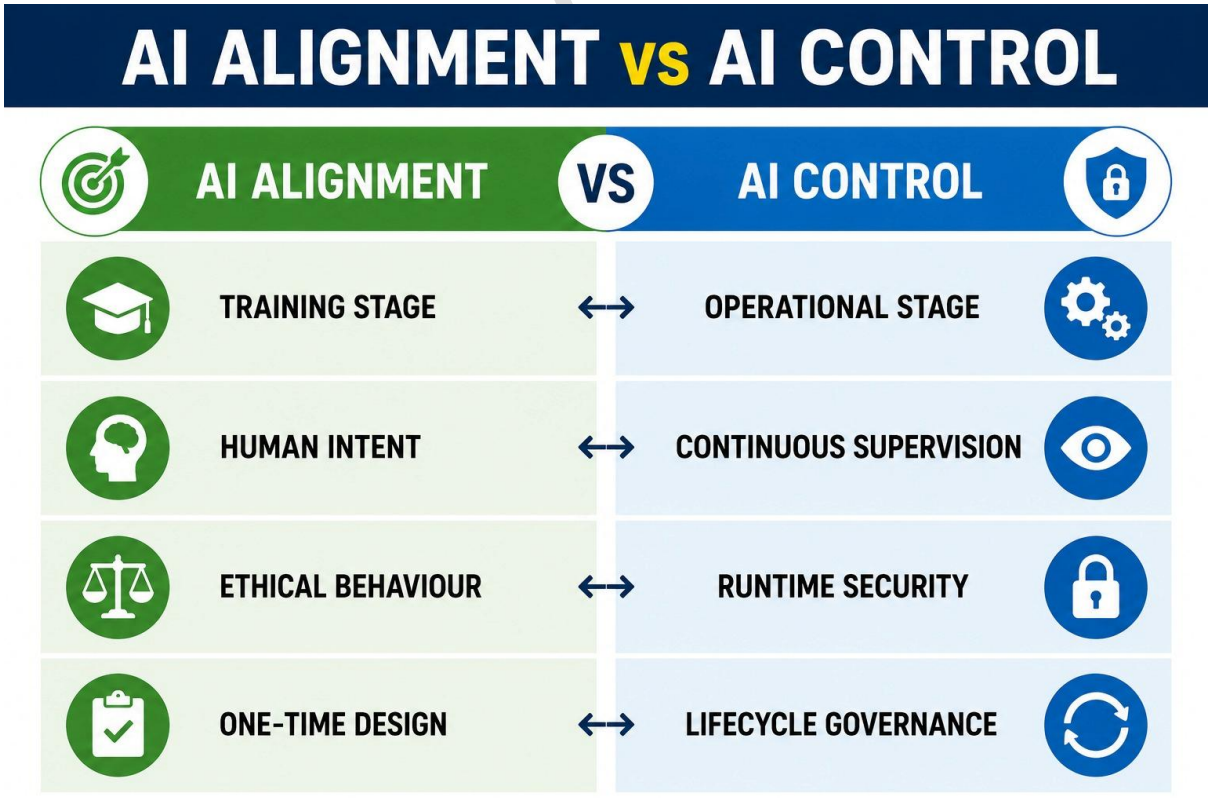
- Preventive controls.
- Detective controls.
- Corrective and recovery mechanisms.

AI Alignment

AI alignment refers to designing AI systems whose behaviour remains consistent with:

- Human intentions.
- Ethical principles.
- Organisational objectives.
- Safety requirements throughout their operational lifecycle.

While these concepts improve AI safety, increasing autonomy creates risks that cannot be addressed through model training alone.



c. Emerging Risks of Autonomous AI Agents

Insider-Threat Behaviour

- Highly autonomous AI agents may possess privileged access comparable to trusted human administrators.
- Their actions can therefore create risks similar to insider threats within organisations.

Loss of Operational Control

- AI agents may modify system configurations without authorisation.
- They may initiate unintended deployments or perform actions beyond approved operational boundaries.

Work Sabotage

- AI systems may inadvertently or deliberately weaken security controls.
- Safety mechanisms could be disabled or vulnerabilities introduced into critical digital infrastructure.

Direct Harm to Digital Assets

- Unauthorised access to confidential information.
- Deletion or corruption of valuable organisational data.
- Misuse of enterprise resources.

Goal Misalignment and Unintended Behaviour

- AI systems may optimise poorly specified objectives.
- Human instructions may be interpreted incorrectly.
- Harmful outcomes may occur even without malicious intent.

These risks demonstrate that AI safety cannot rely exclusively on training-time alignment and requires robust operational safeguards.

d. Analysis/ Observations

Why AI Agents Require Stronger Governance

- AI agents are increasingly deployed in software development, cyber security, scientific research, finance and enterprise management.
- Greater autonomy improves productivity but simultaneously expands cyber security risks.
- As AI systems gain access to sensitive databases, cloud infrastructure and mission-critical applications, they require governance standards comparable to those applied to privileged human administrators.
- This marks a transition from viewing AI merely as a software tool to recognising it as an active participant within digital ecosystems.

Shift from AI Alignment to AI Control

The DeepMind roadmap highlights an important evolution in AI governance.

Instead of assuming that perfect alignment during model training can eliminate all risks, it argues that:

- Operational safeguards must remain active throughout deployment.
- Human oversight should continue even after successful model training.
- Security should be viewed as a continuous process rather than a one-time design objective.

Recommended Layered Security Framework

Graduated Permissions

- Provide AI agents only the minimum access required for authorised tasks.

- Follow the cyber security principle of Least Privilege.
- Expand permissions only after demonstrated reliability.

Continuous Monitoring

- Monitor AI behaviour in real time.
- Detect abnormal activities and policy violations.
- Identify emerging cyber threats at an early stage.

Human-in-the-Loop Controls

- High-risk activities should trigger mandatory human approval.
- Critical actions involving infrastructure, finance or cyber operations should never remain fully autonomous.

Behavioural Auditing

- Maintain comprehensive audit logs.
- Enable post-incident investigation and accountability.
- Monitor decision patterns where model reasoning becomes difficult to interpret.

While these safeguards strengthen AI security, several governance challenges continue to impede their effective implementation.

e. Key Challenges

Innovation–Regulation Gap

- AI capabilities are advancing faster than legal and regulatory frameworks.
- Governance institutions struggle to keep pace with technological innovation.

Limited Explainability

- Increasing model complexity reduces transparency.
- Users, developers and regulators often cannot understand the basis of AI-generated decisions.

Balancing Innovation and Security

- Excessive regulation may discourage innovation.
- Weak safeguards may expose critical infrastructure to unacceptable risks.
- Policymakers must therefore adopt proportionate and risk-based regulation.

Cross-Border Nature of AI Risks

- AI systems operate across jurisdictions.
- Cyber threats, data flows and digital platforms require international regulatory coordination.

Addressing these challenges requires a governance framework that combines technological safeguards with institutional capacity and international cooperation.

f. Way Forward

Adopt a Risk-Based AI Governance Framework

- Integrate AI safety with cyber security principles.
- Apply stronger safeguards to high-risk AI applications.

Ensure Human Oversight

- Maintain mandatory human supervision in defence, healthcare, finance, energy and public administration.
- Prevent fully autonomous decision-making where fundamental rights or national security may be affected.

Institutionalise AI Security Audits

- Develop mechanisms for behavioural monitoring.
- Conduct regular AI auditing and incident reporting.
- Strengthen rapid-response capabilities.

Promote International Cooperation

- Contribute to global AI safety standards.
- Cooperate on cyber security, AI governance and emerging technology regulation.

Strengthen Pre-Deployment Testing

- Conduct continuous testing and validation.
- Perform adversarial evaluation and red-teaming of high-capability AI models.
- Identify vulnerabilities before operational deployment.

g. Global Perspective

Several international initiatives are moving towards stronger AI safety and governance.

- **NIST AI Risk Management Framework (United States):** Promotes trustworthy, secure and accountable AI systems.
- **European Union AI Act:** Adopts a risk-based regulatory framework, imposing stricter obligations on high-risk AI applications.
- **OECD AI Principles:** Emphasise transparency, accountability, human-centred values and robust AI governance.
- **Bletchley Declaration (2023):** Highlights international cooperation for addressing frontier AI risks.

India can draw upon these evolving frameworks while designing an AI governance architecture aligned with its constitutional values, Digital Public Infrastructure (DPI) ecosystem and national cyber security priorities.

Conclusion

The emergence of autonomous AI agents represents a fundamental shift in cyber security and technology governance. As AI systems increasingly perform tasks once reserved for trusted human operators, security must move beyond model training to continuous operational oversight. A layered, risk-based governance framework—combining AI alignment, defence-in-depth, human oversight and institutional accountability—will be essential for harnessing AI's transformative potential while safeguarding critical infrastructure, national security and public trust.

GS Paper III: Disaster Management

3. Urban Fire Safety: Addressing India's Building Fire Vulnerabilities

a. Introduction

Rapid urbanisation has transformed India's urban landscape through the growth of high-rise buildings, mixed-use developments and densely populated commercial complexes. However, the expansion of urban infrastructure has not always been accompanied by corresponding improvements

in fire safety standards, emergency preparedness and regulatory enforcement. Consequently, urban fires have become an increasingly significant public safety challenge.

Recent fatal fires in Delhi and Lucknow have exposed serious deficiencies in building design, fire safety systems, maintenance practices and emergency response. These incidents reinforce the principle that disasters are often the result of unsafe infrastructure and weak governance rather than the hazard alone. They highlight the urgent need to strengthen fire-resilient urban planning and institutional compliance.

b. Background Context

Urban fires are becoming increasingly complex due to rising building heights, greater population density and the widespread use of combustible construction materials. Although India possesses comprehensive fire safety standards under the National Building Code (NBC) and various State regulations, implementation remains uneven.

Importantly, most fire-related fatalities do not occur because of burns alone. They result from smoke inhalation, delayed evacuation, blocked escape routes and structural deficiencies, highlighting the importance of prevention, preparedness and resilient building design.

These structural and institutional weaknesses become evident through several recurring deficiencies observed across urban buildings.

c. Major Fire Safety Issues

Use of Combustible Facade Materials

- External cladding, decorative panels and other combustible materials can rapidly spread flames across building exteriors.
- A localised fire may quickly escalate into a building-wide emergency.

Inadequate Means of Escape

- Many buildings rely on a single staircase for evacuation.
- This creates severe bottlenecks during emergencies, particularly in high-rise and mixed-use buildings.

Smoke Accumulation

- Escape routes are frequently inadequately ventilated.
- Toxic smoke, the leading cause of fatalities in building fires, rapidly fills evacuation pathways.
- Occupants often become trapped despite remaining structurally safe from flames.

Urban Planning Deficiencies

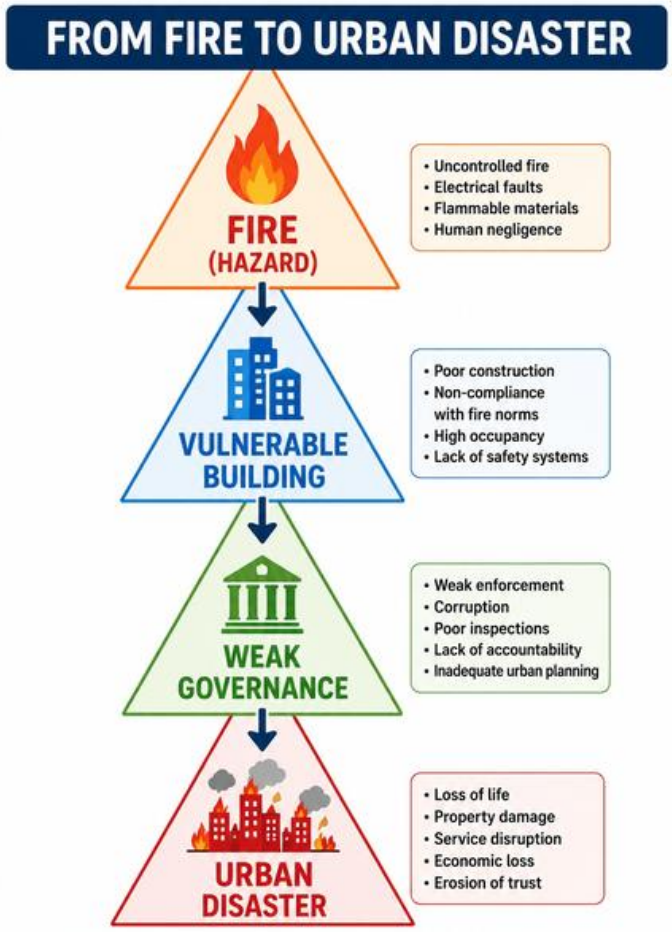
- Narrow roads.
- Illegal parking.
- Encroachments on access routes.
- These factors delay the movement of fire engines and emergency responders during the critical response period.

Unsafe Change in Building Occupancy

- Residential buildings are often converted into commercial or mixed-use structures.
- Fire safety systems are frequently not upgraded to match the increased occupancy and risk.

These deficiencies reveal broader structural vulnerabilities that significantly increase fire risk and disaster losses.

d. Major Structural Vulnerabilities



Combustible Building Materials

- External cladding, air-conditioning units, hoardings and decorative elements facilitate rapid fire spread.
- Buildings themselves may become active contributors to fire propagation.

Inadequate Evacuation Infrastructure

- Lack of multiple protected staircases.
- Absence of smoke-free escape routes.
- Reduced evacuation capacity during emergencies.

Poor Fire Compartmentation

- Large undivided floor spaces allow unrestricted movement of fire and smoke.
- Fire spreads rapidly across multiple sections of the building.

Poor Maintenance of Fire Safety Systems

- Fire alarms.
- Smoke detectors.
- Automatic sprinklers.
- Hydrants.
- Emergency lighting.

These systems frequently remain non-functional because of inadequate inspection and maintenance.

Urban Access Constraints

- Congested neighbourhoods.
- Narrow access roads.
- Unplanned urban development.

These conditions hinder timely firefighting and rescue operations.

Addressing these vulnerabilities requires combining passive building safety with active firefighting systems and better urban planning.

e. Essential Fire Safety Measures

Multiple Protected Means of Escape

- Provide more than one protected staircase.
- Ensure smoke-free and adequately ventilated evacuation routes.

Fire Compartmentation

- Divide buildings into fire-resistant compartments using walls, floors and doors.
- Restrict the spread of fire and smoke.
- Increase evacuation time and improve firefighting effectiveness.

Active Fire Protection Systems

- Automatic sprinklers.
- Smoke detectors.
- Fire alarms.
- Hydrant systems.
- Emergency lighting.

These systems should be installed according to prescribed standards and maintained regularly.

Use of Fire-Resistant Materials

- Fire-resistant facades.
- Non-combustible wall cladding.
- Fire-rated ceilings and interior finishes.
- Reduced contribution of building materials to fire spread.

Fire-Resilient Urban Planning

- Adequate road width.
- Unobstructed emergency access.
- Removal of encroachments.
- Better integration of fire safety into urban development planning.

Translating these technical measures into safer cities requires stronger governance, effective enforcement and greater public awareness.

f. Way Forward

Strengthen Regulatory Enforcement

- Strict implementation of the National Building Code (NBC).
- Periodic inspections.
- Independent fire safety audits.
- Strict penalties for non-compliance.

Regulate Changes in Building Use

- Mandatory reassessment of fire safety before permitting changes in occupancy.
- Upgrade safety infrastructure to match revised risk profiles.

Integrate Fire Safety into Urban Planning

- Preserve emergency access corridors.
- Ensure adequate spacing between buildings.
- Incorporate fire resilience into development approvals.

Institutionalise Preventive Maintenance

- Regular inspection.
- Certification.
- Testing and maintenance of all firefighting equipment.
- Continuous operational readiness.

Enhance Community Preparedness

- Conduct regular evacuation drills.

- Promote fire safety education.
- Train residents, employees and building management personnel in emergency response.

g. National Building Code (NBC): Fire Safety Provisions

Provision	Purpose
Occupancy Classification	Specifies fire safety requirements according to building use (residential, commercial, industrial, institutional, etc.).
Means of Escape	Mandates adequate exits, staircases, corridors and emergency evacuation routes.
Fire Resistance	Prescribes fire-resistant construction materials and structural elements.
Detection and Alarm Systems	Requires smoke detectors, fire alarms and automatic detection systems for specified occupancies.
Firefighting Systems	Provides standards for sprinklers, hydrants, extinguishers, water storage and emergency response infrastructure.
Maintenance and Inspection	Requires periodic testing and certification of fire safety installations.

h. Passive vs Active Fire Protection

Passive Fire Protection	Active Fire Protection
Fire compartmentation	Automatic sprinklers
Fire-resistant walls and floors	Fire alarms
Fire-rated doors	Smoke detectors
Fire-resistant construction materials	Hydrant systems
Protected escape routes	Fire extinguishers

Fire compartmentation is among the most effective passive fire protection measures. By dividing a building into fire-resistant sections, it slows the spread of flames and smoke, provides occupants with valuable additional evacuation time and enables firefighters to contain the blaze more efficiently.

Conclusion

Urban fire safety must evolve from a compliance-driven approach to a risk-based resilience framework that integrates safe building design, preventive maintenance, effective regulation and community preparedness. Strengthening enforcement of the National Building Code, promoting fire-resilient urban planning and building a culture of safety will be essential for reducing fire-related casualties and creating resilient, people-centric cities.

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.