



THE INSTITUTE OF
Company Secretaries of India
भारतीय कम्पनी सचिव संस्थान
IN PURSUIT OF PROFESSIONAL EXCELLENCE
Statutory body under an Act of Parliament
(Under the jurisdiction of Ministry of Corporate Affairs)

SUPPLEMENT PROFESSIONAL PROGRAMME

for

December, 2026 Examination

(Containing updates from June 01, 2025 to May 31, 2026)

ARTIFICIAL INTELLIGENCE, DATA ANALYTICS AND CYBER SECURITY – LAWS & PRACTICE

GROUP 1

ELECTIVE PAPER 4.4

Disclaimer: This document has been prepared for academic purposes only and it does not necessarily reflect the views of ICSI. Any person wishing to act on the basis of this document should do so only after cross checking with the original source.

INDEX

Lesson no.	Lesson Name	Page no.
2	Cyber Security	3
3	Cyber Threats and Cyber Laws	4
5	Regulatory Framework on AI, Cyber Security and Cyberspace	6

Students appearing in Examination shall note the following:

Students appearing in June, 2026 Examination should also update themselves on all the relevant Notifications, Circulars, Clarifications, Orders etc. issued by Ministry of Electronics and Information Technology & Central Government/Regulatory Authorities upto May, 2026.

The students are advised to acquaint themselves with the subject specific updates published in Student Company Secretary Journal by the Institute.

This supplement is to be read with the AIDACS-LP study material (Syllabus 2022) updated up to May, 2025.

LESSON 2

CYBER SECURITY

Digital Personal Data Protection (DPDP) Rules, 2025 (November 17, 2025)¹

Key provisions of the Digital Personal Data Protection (DPDP) Rules, 2025 include:

- **Phased implementation:** an 18-month compliance window, mandatory clear consent notices, and India-based Consent Managers.
- **Breach notification:** timely, plain-language communication to affected individuals.
- **Transparency/accountability:** mandatory contact information, audits and impact assessments for Significant Data Fiduciaries, and government directions on restricted data categories.
- **Data Principal rights:** access, correction, updating, erasure, and nomination of a representative, with a 90-day response mandate.
- **Digital-First Board:** a four-member, fully digital Data Protection Board with online complaint filing; appeals go to TDSAT.

Individual Rights

The Rules empower citizens with rights to consent/withdrawal, information about data use, access, correction, updating, erasure, nomination of a representative, breach notification, and a clear grievance contact — with special protections for children (verifiable parental consent) and persons with disabilities (guardian consent).

Alignment with the RTI Act

The DPDP Act amends Section 8(1)(j) of the RTI Act, reflecting the Puttaswamy privacy judgment, to balance privacy with transparency, without preventing disclosure, only requiring careful assessment. Section 8(2) of the RTI Act remains operative, allowing disclosure where public interest outweighs harm.

¹ <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2190655®=3&lang=2n>

LESSON 3

CYBER THREATS AND CYBER LAWS

Government notified amendments to Rule 3(1)(d) of the IT Rules, 2021 to enhance transparency, accountability and safeguards (October 23, 2025)²

The Ministry of Electronics and Information Technology (MeitY) has notified the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2025 to amend the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (“IT Rules, 2021”). These amendments strengthen the framework of due diligence obligations of intermediaries under the Information Technology Act, 2000 (“IT Act”). Specifically, the amendments to Rule 3(1)(d) introduce additional safeguards to ensure that removal of unlawful content by intermediaries is carried out in a transparent, proportionate and accountable manner. The amended Rules came into effect from 15th November, 2025.

Rule 3(1)(d)³ provides that an intermediary, on whose computer resource the information which is used to commit an unlawful act which is prohibited under any law for the time being in force in relation to the interest of the sovereignty and integrity of India; security of the State; friendly relations with foreign States; public order; decency or morality; in relation to contempt of court; defamation; incitement to an offence relating to the above, or any information which is prohibited under any law for the time being in force is hosted, displayed, published, transmitted or stored shall, upon receiving the actual knowledge under clause (b) of sub-section (3) of section 79 of the Act on such information, remove or disable access to such information within thirty-six hours of the receipt of such actual Knowledge, and such actual knowledge shall arise only in the following manner, namely:—

(i) by an order of a court of competent jurisdiction; or

(ii) a reasoned intimation, in writing, -

(I) issued by an officer authorised for the purpose of issuing such intimation by the Appropriate Government or its agency, being not below the rank of Joint Secretary or an officer equivalent in rank or where an officer at such rank is not appointed, a Director or an officer equivalent in rank, to the Government of India or to the State Government, as the case may be, and, where so authorised, acting through a single corresponding officer in its authorised agency, where such agency is so appointed: Provided that where such intimation is to be issued by the police administration, the authorised officer shall not be below the rank of Deputy Inspector General of Police, especially authorised by the Appropriate Government in this behalf: Provided further that all such intimations shall be subject to periodic review by an officer not below the rank of the Secretary of the concerned Appropriate Government once in every month to ensure that such intimations are necessary, proportionate, and consistent with clause (b) of sub-section (3) of section 79 of the Act and this clause;

² <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2181719>

³ <https://www.meity.gov.in/static/uploads/2026/03/824844a3b380467666137d39149ac47e.pdf>

(II) clearly specifying the legal basis and statutory provision invoked, the nature of the unlawful act, and the specific uniform resource locator, identifier or other electronic location of the information, data or communication link required to be removed or disabled;

Key Highlights of the Amendment Rules are as under:

1. Senior-level Authorisation:

- Any intimation to intermediaries for removal of unlawful information can now only be issued by a senior officer not below the rank of Joint Secretary, or equivalent, or, where such rank is not appointed, a Director or an officer equivalent in rank—and, where so authorised, acting through a single corresponding officer in its authorised agency, where such agency is so appointed.
- In case of police authorities, only an officer not below the rank of Deputy Inspector General of Police (DIG), specially authorised, can issue such intimation.

2. Reasoned Intimation with Specific Details:

- The intimation must clearly specify the legal basis and statutory provision, the nature of the unlawful act, and the specific URL/identifier or other electronic location of the information, data or communication link (“content”) to be removed.
- This replaces the earlier broad reference to ‘notifications’ with ‘reasoned intimation’ to align the Rules with the requirement of ‘actual knowledge’ as mandated under section 79(3)(b) of the IT Act, bringing clarity and precision.

3. Periodic Review Mechanism:

- All intimations issued under Rule 3(1)(d) will be subject to a monthly review by an officer not below the rank of Secretary of the Appropriate Government.
- This ensures that such actions remain necessary, proportionate, and consistent with law.

4. Balance of Rights and Responsibilities:

- The amendments strike a balance between the constitutional rights of citizens and the legitimate regulatory powers of the State, ensuring that enforcement actions are transparent and do not lead to arbitrary restrictions.

5. Expected Impact

- **Transparency & Accountability:** Clear guidelines on who can issue directions and how, with periodic review, ensures checks and balances.
- **Clarity for Intermediaries:** By mandating detailed and reasoned intimations, intermediaries will have better guidance to act in compliance with law.
- **Safeguards and Proportionality:** The reforms ensure proportionality and uphold the principles of natural justice while reinforcing lawful restrictions under the IT Act, 2000.

LESSON 5

REGULATORY FRAMEWORK ON AI, CYBER SECURITY AND CYBERSPACE

MeitY Unveils India AI Governance Guidelines under IndiaAI Mission to Ensure Safe, Inclusive, and Responsible Adoption of Artificial Intelligence across Sectors (November 05, 2025)⁴

The Ministry of Electronics and Information Technology (MeitY), under the India AI Mission, unveiled the India AI Governance Guidelines, a comprehensive framework to ensure safe, inclusive, and responsible AI adoption across sectors. The guidelines propose a robust governance framework to foster cutting edge innovation, and safely develop and deploy AI for all while mitigating risks to individuals and society. The framework comprises four key components:

- Seven guiding principles (Sutras) for ethical and responsible AI.
- Key recommendations across six pillars of AI governance.
- An action plan mapped to short, medium, and long-term timelines.
- Practical guidelines for industry, developers, and regulators to ensure transparent and accountable AI deployment.

India AI Governance Guidelines 2026⁵

The India AI Governance Guidelines (AI Impact Summit 2026) build on seven guiding Sutras and six pillars as recommended by the Committee. They are as under:

1. The Seven Sutras

The framework's guiding principles are designed for cross-sectoral applicability and technology neutrality, providing a flexible and future-ready foundation for responsible AI development and deployment:

- **Trust is the Foundation:** trust must be embedded across the value chain, in technology, developers, supervisory institutions, and users, as the basis for AI adoption at scale.
- **People First:** AI systems must strengthen human agency, retain meaningful human oversight, and reflect societal values, alongside capacity building and safety considerations.
- **Innovation over Restraint:** responsible innovation should generally be prioritised over cautionary restraint, provided harm is minimised.
- **Fairness and Equity:** AI systems should be designed and evaluated to avoid bias and discrimination, particularly against marginalised communities, while actively advancing inclusion.
- **Accountability:** developers and deployers must remain visible and accountable, with obligations assigned according to function, risk of harm, and due diligence.

⁴ <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2186639®=3&lang=2>

⁵ <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2225069®=3&lang=2>

- **Understandable by Design:** explainability and disclosure should be a core design feature, helping users and regulators understand how systems work and what outcomes to expect.
- **Safety, Resilience and Sustainability:** AI systems should be robust, able to detect anomalies, and developed in an environmentally responsible and resource-efficient manner.

Together, these seven principles establish a coherent and balanced AI governance framework that enables innovation while safeguarding trust, equity, and accountability, providing a strong foundation for responsible AI adoption at scale.

2. Six Pillars of Recommendations

1. **Infrastructure:** expanding compute/data access via IndiaAI Mission, promoting locally relevant datasets, integrating AI with Digital Public Infrastructure.
2. **Capacity Building:** scaling programs like IndiaAI FutureSkills and YUVA AI for All, training regulators and law enforcement, extending skilling to Tier-2/3 cities.
3. **Policy and Regulation:** using existing laws (DPDP Act 2023, IT Rules) as a base while closing gaps around liability, content authentication, and copyrighted training data.
4. **Risk Mitigation:** addressing misinformation, bias, deepfakes (especially risks to children and women), and mandating human oversight in sensitive sectors.
5. **Accountability:** graded, risk-proportionate obligations, audits, transparency reports, and stronger grievance redressal.
6. **Institutions:** creating three new bodies: the AI Governance Group (AIGG), the Technology & Policy Expert Committee (TPEC), and the IndiaAI Safety Institute.

3. Action Plan

- **Short term:** Establish key governance institutions, including the AI Governance Group (AIGG)/ Technology and Policy Expert Committee (TPEC), build risk classification frameworks, publish a master circular, expand infrastructure access.
- **Medium term:** common standards on authentication/fairness/cybersecurity, a national AI incidents database, legal amendments, regulatory sandboxes.
- **Long term:** continuous review, new laws for emerging risks, and expanded global diplomatic engagement and contribution to international standards, and horizon-scanning and scenario planning to prepare for future risks and opportunities.

4. Practical Guidelines

For Industry: Companies must comply with applicable Indian laws (IT, data protection, copyright, consumer protection, and protections for women, children, and vulnerable groups) and demonstrate this when required. They should adopt voluntary measures on privacy, security, fairness, and transparency; set up grievance redressal mechanisms; publish transparency reports on India-specific risks; and explore techno-legal solutions like privacy-enhancing tech, machine unlearning, and bias detection.

For Regulators: Agencies should balance innovation support with risk mitigation, keeping frameworks flexible and reviewable. Interventions should target real, present harm rather than pre-emptive restriction. The guidelines caution against heavy compliance burdens like mandatory licensing, favouring the least burdensome effective instrument (codes, standards, advisories, or rules) and encouraging techno-legal approaches to meet policy goals.