ARTICLE

Cybersecurity and Data Protection Compliance: The Practising Company Secretary as the Vanguard of Corporate Cyber Governance

Rapid technological advancement and the advent of AI have triggered a major paradigm shift, forcing traditional law to catch up and redefine professional roles. For the PCS, this transition presents an unprecedented opportunity. As data privacy becomes a boardroom priority, navigating complex compliance mandates falls squarely within the PCS's domain. To remain highly relevant amidst these growing advancements, the modern PCS must transcend traditional administration, adapt to changing corporate needs, and evolve into a techno-legal expert.

CS Rajiv Malik, ACS
Legal Leader, LG Electronics India Ltd.
Greater Noida
rajivmalik09@gmail.com

INTRODUCTION

THE CYBER GOVERNANCE IMPERATIVE

Corporate governance has traditionally been associated with financial discipline, statutory compliance, board processes, and ethical decision-making. However, in today's digital economy, another dimension has silently entered the boardroom: cybersecurity and data protection governance.

A decade ago, cyber incidents were largely perceived as technical disruptions to be handled by IT teams. Today, they have become board-level concerns capable of impacting enterprise value, investor confidence, regulatory standing, customer trust, and even organisational continuity. A ransomware attack can paralyse hospital systems, a data leak can damage corporate reputation overnight, and a delayed regulatory disclosure can expose management to severe financial and legal consequences.

This transformation has significantly altered the expectations from governance professionals, including the practising Company Secretary (PCS).

CYBER COMPLIANCE IS NO LONGER AN IT PROJECT

One of the most significant governance misconceptions within organisations is the belief that cybersecurity and data protection are issues to be addressed exclusively by the IT department. In practice, however, most major cyber incidents expose failures far beyond technology systems. In many organisations, cybersecurity discussions begin only after a disruptive incident occurs. Compliance teams frequently operate in silos separate from technology teams. Human Resources departments may not be adequately aligned with data retention obligations. Procurement functions may onboard vendors without sufficient cybersecurity due diligence. Employees continue to remain vulnerable to phishing and social engineering attacks despite technological safeguards.

This fragmented approach is increasingly incompatible with India's evolving regulatory framework. Compliance today requires coordination between legal, compliance, IT, HR, procurement, internal audit, risk management, and senior leadership teams.

This is where the role of the PCS becomes particularly significant. The PCS, by virtue of their understanding of governance processes, board structures, regulatory accountability, and institutional documentation, is uniquely positioned to act as a coordinating professional between management, technology teams, external consultants, and the board.

THE REGULATORY LANDSCAPE: A MULTI-LAYERED FRAMEWORK

a. GDPR and Concurrent Applicability of Data Protection Laws

Before the Digital Personal Data Protection Act, 2023, Indian organisations processing personal data of individuals located in the European Union were already subject to the General Data Protection Regulation (GDPR), owing to its extra-territorial scope. The GDPR also applies to non-EU entities that offer goods or services to EU data subjects or monitor their behaviour, making compliance mandatory for many Indian companies engaged in cross-border operations. With the introduction of the DPDP Act, such entities now face a regime of concurrent applicability, under which both GDPR and DPDP obligations may apply simultaneously depending on the geographical location of the data subjects.

b. The Digital Personal Data Protection Act, 2023 and DPDP Rules, 2025

The DPDP Act, enacted on 11 August 2023, represents India's first comprehensive standalone data protection legislation. It received Presidential assent after a sustained legislative journey that traced its roots to the Supreme Court's landmark 2017 *Puttaswamy judgment* affirming privacy as a fundamental right under Article 21 of the Constitution. The DPDP Rules, notified by the Ministry of Electronics and Information Technology (MeitY) on 13 November 2025, operationalised the Act through a phased implementation schedule with full compliance expected by 13 May 2027.

The Act's core architecture rests on the following pillars:

- **Data Fiduciary and Data Processor Dichotomy:** Any entity determining the purpose and means of processing digital personal data is a "Data Fiduciary" and bears the primary compliance burden. Entities processing data on behalf of Data Fiduciaries are "Data Processors" and carry secondary obligations.
- **Consent as the Primary Lawful Basis:** Unlike the GDPR's six lawful bases, the DPDP Act centres consent as the primary lawful basis for data processing. Consent must be free, specific, informed, unconditional, and unambiguous. The Rules mandate that consent requests be accompanied by a standalone privacy notice in plain language, available in languages listed in the Eighth Schedule of the Constitution of India.
- **Data Principal Rights:** The Act confers on individuals the right to access their personal data, seek correction, request erasure, nominate a representative for post-mortem data management, and raise grievances. Data Fiduciaries must address grievances within 90 days through a publicly accessible mechanism.
- **Breach Notification:** Organisations must notify both the Data Protection Board of India and affected individuals of any personal data breach 'without delay' upon becoming aware of it. The Rules refine this obligation by mandating a detailed report to the Board within 72 hours.
- **Significant Data Fiduciaries (SDFs):** The Central Government may designate certain entities as SDFs based on volume and sensitivity of data processed, national security implications, and risk to Data Principals. SDFs face enhanced obligations, including appointing an India-based Data Protection Officer (DPO), engaging an independent data auditor, and conducting Data Protection Impact Assessments (DPIAs).
- **The penalty framework is significant:** The Data Protection Board may impose penalties of up to Rs. 250 crore per breach, determined by the nature, gravity, and duration of the violation, and the entity's compliance history. This financial exposure makes proactive compliance not merely a regulatory obligation but a fiduciary duty of the Board of Directors (BOD).

Notably, unlike the GDPR, the DPDP Act applies exclusively to digital personal data collected in digital form or subsequently digitised and does not distinguish between personal and sensitive personal data. The Act also follows a "negative list" approach to cross-border data transfers: personal data may flow to any country except those specifically restricted by the Central Government, of which none had been notified as of February 2026.

Prior to the DPDP Act, India's data privacy framework rested on the Information Technology Act, 2000 and its IT (SPDI) Rules, 2011. To prevent a compliance vacuum, these legacy SPDI Rules remain active as a transitional buffer until ***May 2027***.

> The integration of Artificial Intelligence into corporate workflows has shifted boardrooms toward Agentic Governance, where AI systems act as active participants in record-keeping, board pack synthesis, and automated minute-taking.

c. CERT-In Directions, 2022: Incident Reporting and Operational Mandates

On 28 April 2022, the Indian Computer Emergency Response Team (CERT-In), operating under MeitY pursuant to Section 70B(6) of the Information Technology Act, 2000, issued sweeping cybersecurity directions applicable to service providers, intermediaries, data centres, body corporates, cloud service providers, VPN providers, virtual private server operators, and virtual asset service providers. These directions introduced what is arguably the world's most demanding mandatory incident reporting timeline.

The principal obligations under the CERT-In Directions include:

1. **Six-Hour Mandatory Reporting:** Covered entities must report specified categories of cybersecurity incidents to CERT-In within six hours of detecting or becoming aware of the incident. Crucially, the trigger is detection or awareness not forensic validation or impact assessment. This means organisations must have pre-built incident triage procedures capable of generating a preliminary report within hours of initial detection.
2. **Log Retention for 180 Days:** All entities must maintain logs of their Information and Communication Technology (ICT) systems for a

minimum of 180 days and ensure such logs are stored within India. These logs must be provided to CERT-In upon request or when reporting an incident.

3. **Designated Point of Contact:** Each covered entity must appoint a designated Point of Contact (PoC) to interface with CERT-In for compliance purposes, incident reporting, and receipt of advisories.

4. **KYC for Service Providers:** All service providers must maintain verified Know Your Customer (KYC) records of their subscribers/customers for a minimum period of five years.

The CERT-In Directions represent a profound shift in the compliance orientation of corporate India. Non-compliance attracts criminal penalties under the IT Act, including imprisonment of up to one year and/or fine.

d. SEBI's Cybersecurity and Cyber Resilience Framework (CSCRF), 2024

The Securities and Exchange Board of India issued the CSCRF circular on 20 August 2024, consolidating a decade of fragmented circulars into a unified, risk-based governance framework. The CSCRF applies to all SEBI Regulated Entities (REs), encompassing stock exchanges, depositories, clearing corporations, mutual funds/AMCs, stock brokers, depository participants, portfolio managers, investment advisers, KYC Registration Agencies, and venture capital funds.

The CSCRF classifies REs into five tiers, namely: Market Infrastructure Institutions (MIIs), Qualified REs, Mid-Size REs, Small-Size REs, and Self-Certification REs; obligations are calibrated to each tier's scale and systemic importance. The framework's most significant governance innovation is its elevation of cybersecurity to board-level responsibility: SEBI now requires BOD of financial entities to conduct quarterly reviews of cyber risk posture, approve cybersecurity budgets, and sign off on the designation of critical systems and data classification frameworks.

Source: *Self-created by author as per SEBI CSCRF (reference 5)*

e. RBI Master Direction on IT Governance, Risk, Controls and Assurance Practices, 2023

The Reserve Bank of India (RBI) established a definitive sectoral standard for financial institutions through its *Master Direction on IT Governance, Risk, Controls and Assurance Practices*, which took effect on April 1, 2024. This framework firmly shifts IT governance into the core corporate governance domain, placing ultimate accountability for technology strategy and security directly on the BOD. Under this mandate, Regulated Entities (REs) must establish a Board-level IT Strategy Committee (ITSC). Chaired by an independent director, the ITSC must meet at least quarterly to ensure that digital investments and tech risks align seamlessly with the institution's broader business objectives.

Operationally, the Master Direction enforces structural independence through a strict segregation of duties. Organisations must appoint a Chief Information Security Officer (CISO) at a senior management tier, reporting directly to the Executive Director or Head of Risk, completely separate from the standard IT delivery department. The framework demands a comprehensive risk-management approach, requiring a robust Information Security Management System (ISMS) alongside regular Vulnerability Assessment and Penetration Testing (VAPT) to protect critical infrastructure. Furthermore, third-party exposures face tight regulatory oversight; the BOD and senior management remain legally accountable for outsourced operations, making "Right to Audit" clauses a mandatory feature in all material IT vendor contracts.

FROM LEGAL AWARENESS TO IMPLEMENTATION READINESS

For many organisations, the immediate response to emerging cybersecurity and data protection regulations is the preparation of policies, notices, and compliance documentation. While documentation remains an essential starting point, practical experience increasingly demonstrates that cyber compliance cannot be achieved through paperwork alone. The real challenge lies in implementation readiness.

In several organisations, particularly those undergoing rapid digital transformation, technology adoption has progressed faster than governance integration. Cloud-based platforms, AI-enabled tools, digital HR systems, customer analytics platforms, mobile applications, remote working environments, and third-party SaaS ecosystems have become deeply embedded into business operations. However, internal governance structures governing data accountability, retention protocols, access management, incident escalation, and vendor oversight often continue to evolve reactively rather than strategically. As a result, organisations frequently encounter implementation gaps not because regulations are unclear, but because institutional coordination remains fragmented.

One of the most common practical challenges is the disconnect between technology functions and compliance functions. IT teams may focus on system functionality and operational continuity, while legal and compliance teams focus on regulatory interpretation and documentation

requirements. In the absence of coordinated governance structures, critical areas such as consent management, breach response, employee awareness, and vendor accountability may remain inadequately aligned.

Cyber governance, therefore, requires a shift from isolated departmental ownership to enterprise-wide accountability.

From a practical implementation perspective, organisations increasingly need to focus on five interconnected pillars:

(a) Legal Scoping and Data Mapping

Implementation begins with understanding the organisation's data ecosystem. Many businesses continue to underestimate the extent of personal data processed across internal systems, vendor platforms, archived records, marketing databases, and employee management tools.

Data frequently exists across multiple business functions without central visibility regarding:

- Purpose of processing;
- Retention timelines;
- Access controls;
- Cross-border transfers;
- Vendor dependencies; and
- Deletion protocols.

A structured legal scoping exercise helps organisations identify:

- Categories of personal data processed;
- Business processes involving data flows;
- Applicable regulatory obligations;
- High-risk processing activities; and
- Areas requiring remediation.

In practical terms, this stage often becomes the foundation upon which the entire compliance framework is built.

(b) Governance Structures and Internal Accountability

Cybersecurity governance cannot function effectively without clearly defined accountability structures. One emerging best practice is the establishment of cross-functional implementation task forces involving representatives from:

- Legal and compliance;
- IT and information security;
- HR;
- Procurement;
- Internal audit;
- Risk management; and
- Business operations.

Such coordination mechanisms help ensure that compliance obligations are translated into operational processes rather than remaining confined to policy documents.

Equally important is the establishment of internal escalation frameworks. During cyber incidents, delays frequently arise because organisations lack clarity regarding:

- Who must be informed?
- Who evaluates materiality?
- Who interfaces with regulators?
- And who communicates with management and the board?

In a regulatory environment where certain incidents may require reporting within hours, governance clarity becomes critical.

(c) Training, Awareness, and Organisational Culture

Technology controls alone cannot eliminate cyber risk exposure. In practice, employee behaviour continues to remain one of the most significant vulnerability points for organisations. Phishing attacks, weak password practices, unauthorised data sharing, insecure remote working practices, and inadvertent disclosure of confidential information continue to contribute significantly to cyber incidents globally.

Consequently, organisations must move beyond one-time awareness sessions and create continuous sensitisation frameworks.

Effective cyber governance increasingly requires:

- Periodic employee awareness programmes;
- Role-based training modules;
- Senior management sensitisation;
- Simulated phishing exercises;
- Incident reporting awareness; and
- A periodic review of internal practices.

Importantly, cybersecurity culture must flow from the top. BOD and senior management teams that visibly prioritise cyber governance often create stronger institutional accountability across the organisation.

(d) Vendor Ecosystems and Third-Party Risks

Modern enterprises operate through interconnected digital ecosystems. Payroll processors, cloud service providers, HR management platforms, customer engagement vendors, analytics providers, consultants, and outsourced support functions may all process organisational or personal data in some capacity.

In many recent global and Indian cyber incidents, vulnerabilities have originated not within the organisation itself but through third-party service providers. This has significantly increased regulatory focus on vendor governance. Practical implementation, therefore, requires organisations to strengthen:

- vendor onboarding due diligence;
- contractual data protection clauses;
- breach notification obligations;
- audit rights;
- access controls;
- and exit management protocols.

For governance professionals, vendor risk management is rapidly becoming one of the most critical dimensions of cyber compliance oversight.

(e) Continuous Review and Incident Preparedness

Cyber compliance is not a one-time implementation exercise. Regulatory expectations increasingly emphasise continuous preparedness, periodic review, and demonstrable governance maturity. Policies drafted but never tested provide little protection during actual incidents.

As a result, organisations are increasingly expected to conduct:

- periodic risk assessments;
- vulnerability testing;
- mock incident response exercises;
- board-level cyber reviews;
- policy updates;
- and remediation tracking exercises.

Preparedness today is measured not merely by whether organisations possess policies, but by whether they can respond effectively under pressure.

In many ways, the true test of cyber governance begins not before an incident, but during one.

The increasing operational complexity of cyber compliance also highlights a broader professional reality. Organisations today require advisors who can bridge governance expectations with implementation realities. This expanding intersection between regulation, risk management, institutional processes, and board accountability is creating a significant professional opportunity for Practising Company Secretaries.

COMPLIANCE OBLIGATIONS: A PRACTICAL ANATOMY

(The expanding role of PCS)

For the PCS advising corporate clients, cybersecurity and data protection compliance can be practically structured around six interconnected domains: Governance and board accountability; Data lifecycle management; Incident response and breach notification; Third-party and vendor management; Risk Minimisation and last but not the least i.e. AI Governance and Techno-Legal.

a. Governance and Board Accountability

The most significant paradigm shift in India's emerging cyber regulatory framework is the explicit imposition of board-level responsibility.

Practical governance actions include:

- **Board-Approved Cybersecurity Policy:** Every corporate entity should have a board-approved Cyber Security and Data Protection Policy that addresses the DPDP Act's consent framework, breach notification obligations, data retention schedules, and data principal rights.
- **Cyber Risk as a Board Agenda Item:** It is recommended to add Cyber Risk as a Board-level Agenda item to strengthen cyber governance. The PCS should institutionalise cyber risk as a standing item on the risk committee and main board agenda.
- **Appointment of DPO and CERT-In PoC:** The DPDP Act mandates the appointment of an India-based DPO for SDFs. CERT-In Directions require a designated Point of Contact for all covered entities. The PCS can advise on the qualifications, appointment process, and documented governance charter for these roles.
- **Annual Report Disclosures:** The Board's Report under the Companies Act, 2013 and SEBI LODR Regulations must increasingly reflect an organisation's cyber risk profile, incidents, and compliance posture. The PCS should ensure that disclosures are accurate, complete, and reflective of the organisation's actual state of cyber preparedness.

b. Data Lifecycle Management

The DPDP Act's principle of "storage limitation" requires that personal data be retained only for as long as necessary for the purpose for which it was collected. Upon purpose fulfilment or consent withdrawal, data must be deleted.

The data lifecycle compliance programme should encompass:

- **Data Inventory and Mapping:** A comprehensive register of all personal data assets, including their origin, purpose, legal basis, storage location (including third-party processors and cloud infrastructure), and applicable retention period.
- **Privacy Notices and Consent Mechanisms:** Under the DPDP Rules, privacy notices must be standalone, in plain language, and available in all 22 scheduled languages of India. Consent mechanisms must be purpose-specific and easily withdrawable. Legacy data collected before the Rules came into force requires retrospective notices to be issued within the compliance window ending 13 May 2027.

- **Data Retention and Erasure Schedules:** Automated data lifecycle policies to delete data upon purpose fulfilment or consent withdrawal are mandated by the DPDP Act. In practice, this requires integration between legal compliance requirements and the organisation's IT/ERP systems.
- **Data Protection Impact Assessment (DPIA) for High-Risk Processing:** SDFs and any entity engaging in processing likely to result in high risk to data principals, large-scale processing of children's data, profiling, systematic monitoring should conduct DPIAs as a pre-emptive governance tool.

c. Incident Response and Breach Notification

Breach notification is arguably the most operationally demanding compliance requirement of the current regulatory framework. As a practical matter, meeting the CERT-In six-hour standard, which is the shortest in the world, requires that organisations have invested in detection and response infrastructure well before an incident occurs. The PCS plays a vital role in ensuring the following organisational capabilities exist:

- An Incident Response Plan (IRP) that is board-approved, CERT-In compliant, and tested through at least annual simulation exercises.
- An internal escalation matrix specifying the sequence of notifications.
- Pre-cleared notification templates for CERT-In reporting, SEBI incident portal submissions, and Data Principal communication, drafted by PCS and approved in advance by legal and compliance counsel.
- A comprehensive post-incident review process to determine root cause, assess regulatory exposure, and implement corrective actions is documented and presented to the board.

The CERT-In framework adopts a "response behaviour" orientation: even well-resourced organisations can attract regulatory scrutiny for procedural failures, while smaller entities with proactive and transparent response mechanisms are treated as compliant. This makes the quality of incident response governance not just the technical sophistication of the organisation the decisive compliance variable.

d. Third-Party and Vendor Risk Management

Modern business operations are inherently dependent upon third-party services: cloud platforms, payroll processors, marketing technology vendors, customer relationship management systems, and a variety of SaaS applications each process organisational data.

A robust third-party risk management programme should include:

- **Vendor Due Diligence:** Pre-onboarding assessment of prospective vendors' data security practices, certifications (ISO 27001 is the industry standard), incident history, and contractual willingness to meet DPDP Act requirements.
- **Data Processing Agreements (DPAs):** All vendor contracts involving personal data processing must include DPDP-compliant DPAs specifying security obligations, permitted processing purposes, breach notification timelines, data deletion upon contract termination, and audit rights of the Data Fiduciary.
- **Periodic Vendor Audits:** Annual or event-triggered security audits of significant vendors, with findings documented and presented to management or the Audit Committee.

e. Risk Minimisation in M&A Transactions

In most M&A transactions, personal data relating to customers, employees, vendors, and other stakeholders is accessed and shared from early diligence stages and often post-closing. Under the DPDP Act's rights-based framework, the sharing of identifiable personal data without lawful purpose, valid consent, or adequate safeguards can expose parties to regulatory risk even before transaction documents are executed, directly affecting data usability and deal value.

Except for limited court-approved restructurings, M&A transactions will increasingly be subject to DPDP compliance obligations. This transition necessitates a governance-led approach to transaction execution.

Deal approvals must now account for the following so as to safeguard the organisations from significant penalties:

- Data protection readiness
- Consent gaps
- Vendor dependencies
- Post-closing data usability
- Integration of data protection principles
- Data minimisation
- Vendor contract oversight
- Breach-response readiness

As regulatory scrutiny intensifies, DPDP preparedness by PCS will become a key determinant of transaction certainty, valuation protection, and sustainable deal execution.

f. AI Governance and the Techno-Legal Architect

The integration of Artificial Intelligence into corporate workflows has shifted boardrooms toward Agentic Governance, where AI systems act as active participants in record-keeping, board pack synthesis, and automated minute-taking. India AI Governance Guidelines (2026) provide a broad framework which can be followed for better governance. For PCS, this evolution demands a transition into a Techno-Legal Architect. It is no longer sufficient to merely interpret statutes; the PCS must validate that automated governance systems are free from systemic bias and accurately reflect the "sense of the meeting".

A PRACTICAL CYBER-COMPLIANCE CHECKLIST FOR PCS

The following checklist distils the foregoing analysis into actionable compliance items that a PCS can use as a

diagnostic tool when onboarding a new client or conducting an annual compliance review. It is organised by the five primary frameworks applicable to corporate entities, including financial entities:

	DPDP Act, 2023 & DPDP Rules, 2025	CERT-In Directions, 2022	SEBI (CSCRF, 2024)	India AI Governance Guidelines, 2026	RBI Master Direction, 2023
1.	Conduct a full data mapping exercise covering all personal data flows.	Appoint a designated CERT-In Point of Contact with documented authority and contact details.	Classify the entity under the CSCRF's five-tier framework to determine specific applicable obligations.	Constitute AI Governance Committee.	Board approval of IT/Cyber policies.
2.	Determine whether the entity qualifies as a Significant Data Fiduciary (SDF).	Implement ICT log retention for 180 days with mandatory India-based storage.	Appoint a CISO at a CTO/ CIO-equivalent level reporting directly to the MD/CEO for MIIs and Qualified REs.	Maintain AI systems inventory.	Quarterly ITSC review compliance tracking.
3.	Draft and implement privacy notices in plain language, ensuring availability in all 22 scheduled languages where required.	Establish a six-hour incident reporting capability encompassing detection, triage, and preliminary reporting.	Establish or join a compliant Security Operations Centre (SOC), or utilize M-SOCs via NSE/BSE for smaller entities.	Classify AI use-cases by risk.	Cyber risk reporting to Board monitored.
4.	Establish and operationalise a robust consent management mechanism.	Draft and obtain board approval for a CERT-In compliant Incident Response Plan.	Obtain mandatory ISO 27001 certification for MIIs and Qualified REs.	Document AI workflows and datasets.	CISO appointment and reporting independence verified.
5.	Appoint a Data Protection Officer (DPO) for SDFs and establish their reporting line and governance charter.	Conduct annual tabletop exercises to test the Incident Response Plan and six-hour reporting infrastructure.	Schedule Vulnerability Assessment and Penetration Testing (VAPT) at prescribed frequencies.	Ensure human oversight for critical AI decisions.	Vendor cyber risk assessment documentation reviewed.
6.	Establish a Data Principal Rights Response mechanism with a 90-day grievance resolution window.		Present quarterly cyber risk reports and budget reviews to the board.	Verify AI compliance with applicable laws.	BCP and DR drill records examined.
7.	Implement a data retention and automated erasure schedule to meet storage limitation requirements.		Maintain all encryption key management operations within India's territorial boundaries.	Conduct AI bias and risk assessments.	VA/PT testing periodicity compliance checked.
8.	Review and update all vendor contracts to include DPDP-compliant Data Processing Agreement (DPA) clauses.		Report cybersecurity incidents to SEBI/CERT-In within six hours and declare a "Disaster" within 30 minutes of critical system disruption.	Establish AI grievance and escalation mechanism.	Audit trail and access control oversight ensured.
9.	Establish a 72-hour detailed breach notification protocol for reporting to the Data Protection Board.			Review AI vendor contracts and data controls.	Incident reporting and escalation mechanism validated.
10.	Issue retrospective notices to all Data Principals whose data was collected before Rules came into force by the 13 May 2027 deadline.			Conduct periodic AI governance audits and training.	IS Audit observations closure monitoring maintained.

CONCLUSION

Rapid technological advancement and the advent of AI have triggered a major paradigm shift, forcing traditional law to catch up and redefine professional roles. For the PCS, this transition presents an unprecedented opportunity. As data privacy becomes a boardroom priority, navigating complex compliance mandates falls squarely within the PCS's domain. To remain highly relevant amidst these growing advancements, the modern PCS must transcend traditional administration, adapt to changing corporate needs, and evolve into a techno-legal expert. By doing so, they can effectively serve as the true vanguard of corporate cyber governance.

REFERENCES:

i. *CERT-In Cyber Security Directions.*

ii. *Digital Personal Data Protection Act, 2023 and Rules thereof.*

iii. *India AI Governance Guidelines (February 2026)*

iv. *Reserve Bank of India, Master Direction – Reserve Bank of India (Information Technology Governance, Risk, Controls and Assurance Practices) Directions, 2023.*

v. *SEBI Circular and SEBI (CSCRF).*