The Institute of Chartered Accountants of India

(Set up by an Act of Parliament)

Women & Young Members Excellence Committee

Organises

SkillUp Knowledge Webinar Series



CA. Purushottam H. Khandelwal
Chairman, WYMEC, ICAI



CA. Sripriya Kumar
Vice Chairperson, WYMEC, ICAI

TECHNICAL CPE SESSION | OCTOBER 2026

Data Audits and DPIAs under DPDPA

A Practical Approach to Privacy Assurance

CA Zalak Parikh

Associate Director | Governance, Risk & Compliance

K C Mehta & Co LLP

FCA | CISA | DISA (ICAI) | FAFD (ICAI) | CCCAB | DPDPA Certified

ISO/IEC 27001, 27701 & 42001 Lead Auditor | AICA Level 1

SESSION ROADMAP

One hour | What we will cover

Regulatory journey

DPDPA timeline and phased implementation

Mandatory audit regime

SDF obligations, Rule 13 and 5 October 2026 Order

CA readiness

Eligibility, independence, engagement and skills

Audit universe

Act and Rule checkpoints, evidence and control tests

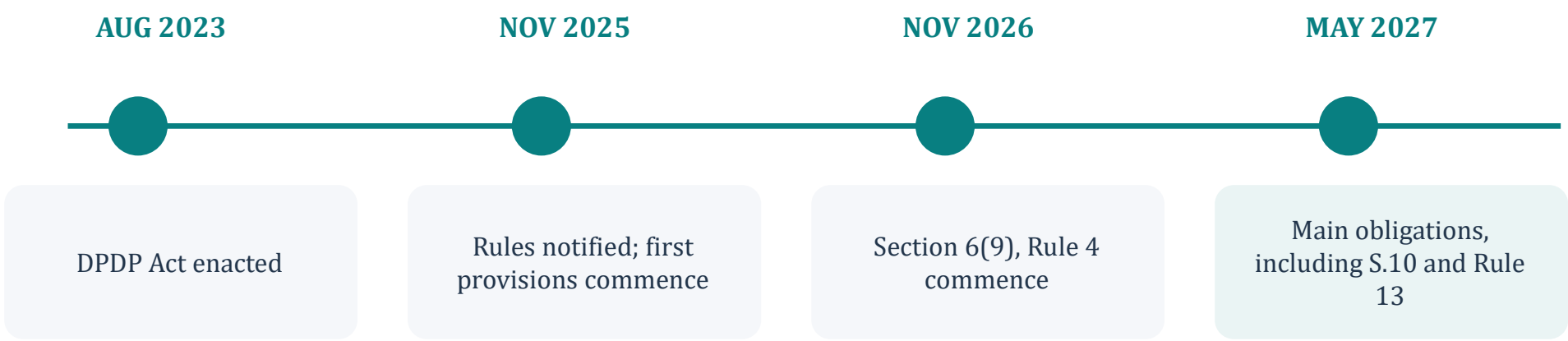
DPIA in practice

Methodology, sample risk assessment and reporting

Closing

Key takeaways and Q&A

DPDPA | The regulatory journey



Plus: Removal of Difficulties Order dated 5 October 2026, published 7 October 2026

What is in force as of 9 October 2026?

ALREADY COMMENCED

Selected Act provisions relating to definitions, the Data Protection Board and enabling architecture.

DPDP Rules 1, 2 and 17 to 21.

The 2026 Removal of Difficulties Order is effective from publication.

FUTURE COMMENCEMENT

November 2026: Section 6(9) and Rule 4.

May 2027: Principal substantive obligations, including Sections 3–10 and Rule 13.

The 12-month SDF audit/DPIA cycle runs from SDF notification, under Rule 13.

Assess readiness now; do not misstate future obligations as already enforceable

Mandatory audit or voluntary assessment?

Notified SDF	**Statutory obligations**	Independent Data Auditor; periodic Data Audit and DPIA; Rule 13 reporting
Other Data Fiduciary	**DPDPA readiness / compliance audit**	Voluntary under DPDPA; sector-specific audit mandates may separately apply
Data Processor	**Processor control assurance**	Verify controls under DF instructions and contract; no universal standalone DPDP audit mandate

Important: SDF status is a government notification, not an entity's self-declared classification.

Who can be notified as a Significant Data Fiduciary?

01

VOLUME & SENSITIVITY

Scale and characteristics of personal data

02

INDIVIDUAL RIGHTS

Risks to Data Principals

03

SOVEREIGNTY

Potential impact on India’s sovereignty and integrity

04

DEMOCRACY

Risk to electoral democracy

05

SECURITY

Security of the State

06

PUBLIC ORDER

Implications for public order

Section 10 | The statutory obligations

A

DATA PROTECTION OFFICER

Appoint India-based DPO, responsible to the board or equivalent governing body.

B

INDEPENDENT DATA AUDITOR

Appoint independent Data Auditor to evaluate SDF compliance with the Act.

C

PERIODIC DPIA + DATA AUDIT

Carry out periodic DPIA, data audit and other prescribed measures.

DPIA statutory elements: Data Principal rights + processing purpose + assessment and management of risks to rights.

Rule 13 | Operationalising the SDF obligation

Rule	Requirement	Audit implication
13(1)	DPIA and audit once in every 12 months from SDF notification	Track notification date, cycle and completed work
13(2)	Report significant observations to the Board	Define escalation and reporting workflow
13(3)	Due diligence on technical measures, including algorithms	Assess potential risks to Data Principal rights
13(4)–(5)	Restrictions for any centrally specified personal data / traffic data	Map cross-border flows; check future specification

“Significant observations” is statutory wording; no fixed audit report format is prescribed here.

MeitY clarification | 5 October 2026 Order

Published in the Official Gazette: 7 October 2026

Section 10(2)(c)(ii)

BEFORE

“periodic audit”

→

AFTER

“periodic data audit”

The Order also corrects wording in Section 9(1) regarding children and persons with disabilities who have lawful guardians.

What the October 2026 clarification means

CLARIFIES

The two audit references in Section 10(2) concern a data protection audit / data audit.

DOES NOT CREATE

A separate audit of financial statements, an IT-only certification, or an audit requirement for all Data Fiduciaries.

DOES NOT SPECIFY

Exclusive qualification for Chartered Accountants, a new audit standard, or a standalone prescribed report format.

PROFESSIONAL RESPONSE

Frame engagements accurately; differentiate statutory SDF audit from voluntary readiness assessments.

Before accepting a Data Audit | CA readiness

1 VERIFY THE MANDATE

SDF notification? Statutory audit or advisory assignment?

2 ASSESS COMPETENCE

Privacy law, data flows, ITGC, cloud, security and third parties

3 CHECK INDEPENDENCE

Conflicts, self-review threats and objectivity

4 AGREE AUDIT CRITERIA

DPDP Act/Rules, applicability matrix and suitable benchmarks

5 DEFINE SCOPE

Systems, locations, entities, processors, exceptions and sampling

6 ESTABLISH EVIDENCE

Access rights, confidentiality, handling, retention and audit trail

Engagement quality | Protect the assurance opinion

BEFORE FIELDWORK

Engagement letter and intended use

Applicable criteria and management assertions

Roles of CA, specialist and client management

Scope exclusions, sampling, timeframe

Evidence security and confidentiality

DURING / AFTER

Professional scepticism and corroboration

Test design versus operational effectiveness

Document sampling and limitations

Management response and remediation owners

Clear conclusion without overstating assurance

Be especially cautious where your firm designed or implemented controls being independently audited.

DPDP Act 2023 | Build your audit universe

Audit domain	Act linkage	Auditor's core question
Applicability and processing	S3, 4, 7	Which digital personal data is processed and on what basis?
Notice and consent	S5, 6	Is the purpose explained and consent demonstrable where needed?
Accountability and processors	S8	Does the Data Fiduciary supervise its processing and vendors?
Children and vulnerable persons	S9	Are applicable protective restrictions implemented?
Data Principal rights	S11–14	Can individuals exercise statutory rights effectively?
Cross-border / special duties	S10, 16	Are SDF and transfer obligations addressed where applicable?

DPDP Rules 2025 | Turn provisions into test steps

Rule(s)	Audit theme	Illustrative evidence
3	Notice	Notice versions, purpose statement, channel screenshots
6	Safeguards	Access matrix, masking, encryption, logs, backups
7	Breach reporting	Incident register, escalation clock, draft intimation
8	Erasure / retention	Retention schedule, deletion jobs, exceptions
10–12	Children / exemptions	Age verification, parental consent, exemption basis
13	SDF additional duties	DPIA, data audit, board report, technical due diligence
14–15	Rights / cross-border	Request workflow, grievances, data hosting maps

Data Audit methodology | A practical six-step cycle

01 **PLAN**

Scope, criteria and legal applicability

02 **MAP**

Personal data, owners and data flows

03 **ASSESS**

Risk and control design

04 **TEST**

Evidence, walkthroughs and samples

05 **REPORT**

Findings, causes and residual exposure

06 **FOLLOW UP**

Action owners, milestones, closure evidence

Sampling and evidence | Ask, inspect, corroborate

Control objective	Evidence request	Test approach
Consent captured	Screen flow, consent DB, audit trail	Trace sampled transactions to recorded consent
Access limited	RBAC matrix, joiner/leaver tickets	Re-perform access sample and test removal
Processor governed	DPA / contract, due diligence, assurance reports	Trace contractual obligations to controls
Breaches handled	Incident log, playbook, detection alerts	Walk through incident and notification decisions
Erasure operated	Retention register, deletion reports	Check triggers, exceptions and deletion proof

Screenshots alone seldom demonstrate sustained operating effectiveness.

Focus area | Notice, consent and individual rights

NOTICE & CONSENT AUDIT

Compare collection fields with itemised notice.

Trace explicit consent where Section 6 applies.

Test withdrawal simplicity and effect.

Review legacy personal data notice readiness and consent record lineage.

DATA PRINCIPAL RIGHTS AUDIT

Test published request and grievance channels.

Check identity verification proportionality.

Trace access, correction and erasure cases.

Check grievance timelines and escalation paths.

Focus area | Security safeguards and breach management

PREVENT
Encryption/masking, access control, privileged access review

DETECT
Logging, monitoring, alert triage and anomalous access

RECOVER
Backups, recovery tests and continuity measures

RETAIN
Rule 6(1)(e): applicable log/data retention baseline; legal exceptions

RESPOND
Incident classification, evidence preservation, escalation

NOTIFY
Data Principal / Board intimation processes; Rule 7 time frames

Focus area | Processors, retention and special data

THIRD-PARTY PROCESSORS

Contracts, instructions, security commitments, cloud/SaaS assurance and sub-processors

RETENTION & ERASURE

Purpose end, withdrawal, statutory exceptions, archive and backup handling

CHILDREN'S DATA

Age/guardian checks, verifiable consent and applicable exemptions

CROSS-BORDER FLOWS

Hosting, support access, transfers, Rule 15 and SDF-specific Rule 13(4) restriction

DPIA | What the DPDPA actually requires

Mandatory periodic DPIA: Notified Significant Data Fiduciaries

1

DESCRIBE

Rights of Data Principals affected

2

EXPLAIN

Purpose of personal data processing

3

ASSESS

Risks to Data Principal rights

4

MANAGE

Measures that address identified risks

The risk matrix and workflow on the next slides are illustrative techniques, not a prescribed statutory template.

DPIA workflow | From processing to residual risk

1	**PROCESS**	Scope, data classes, purposes, recipients
2	**PEOPLE**	Data Principal rights and expected effects
3	**THREATS**	Misuse, overcollection, disclosure, retention
4	**RISK**	Likelihood, impact and existing safeguards
5	**ACTION**	Mitigation, ownership, treatment deadlines
6	**REVIEW**	Residual risk, approvals and re-assessment

Case study | HRMS with cloud payroll processor

ILLUSTRATIVE PROCESSING ACTIVITY

SOURCE
Employees / candidates

→

SYSTEM
Cloud HRMS and payroll

→

PROCESSOR
Payroll SaaS and support

→

OUTPUT
Payslips, statutory filings

Audit question	Evidence
Is each HR data field necessary for the stated purpose?	Data inventory, privacy notice and field dictionary
Who accesses salary, ID and bank information?	Access matrix, logs, approval and leaver evidence
What controls govern the SaaS provider?	Contract, due diligence and security assurances
How are exits, deletion and backups handled?	Retention policy, deletion records and exceptions

Sample DPIA | Map harm to mitigation

Risk to Data Principal	Impact	Example mitigation	Residual position
Excessive HR data collection	Unnecessary exposure	Data minimisation, purpose review	Reassess
Unauthorised payroll access	Financial / identity harm	RBAC, MFA, logging, quarterly reviews	Verify
Uncontrolled support access	Disclosure to third parties	Vendor controls, access expiry, monitoring	Retest
Data retained after purpose ends	Continued privacy risk	Retention schedule and exception register	Track

Likelihood × impact is a useful practice aid; not an official DPIA scoring model.

Write audit findings that management can act on

Illustrative audit observation

Issue | Terminated HRMS users retain active access

- Criteria: access control and security safeguard expectations under Rule 6
- Condition: 4 of 25 sampled leavers retained active accounts
- Cause / exposure: inconsistent offboarding and unauthorised access risk
- Recommendation: automated deprovisioning, owner, due date and retest

Reporting discipline: criterion • condition • cause • risk • recommendation • management response.

SDF reporting | What goes to the Board?

STATUTORY RULE 13(2)

The person carrying out the DPIA and audit must furnish a report containing significant observations to the Data Protection Board.

The Rule does not prescribe a detailed universal report template.

PRACTICAL REPORT CONTENTS

Assignment scope, criteria and limitations

Significant control failures and potential impact

DPIA risk conclusions and residual exposure

Recommendations, owners and deadlines

Management response and follow-up

Agree a defensible “significant observation” threshold; do not substitute “material” as statutory wording.

Five messages for every Chartered Accountant

- Establish whether an SDF statutory mandate exists before describing an audit as mandatory.
- Read Section 10 with Rule 13 regarding 12 month audit cycle.
- Treat privacy audit as a cross-functional legal, technology, operations and governance exercise.
- Demonstrate compliance using reliable evidence, not policies or screenshots alone.
- Keep the Data Audit and DPIA distinct, but align findings and mitigation actions.

THANK YOU

Questions & discussion

CA Zalak Parikh

Associate Director | Governance, Risk & Compliance

K C Mehta & Co LLP