DPDP Act Compliance Assessment

Sample Board & CEO Report — XYZ Foundation (fictional organisation)

Illustrative sample – fictional organisation. XYZ Foundation does not exist. Every answer, score and finding in this report was invented to show what the toolkit produces. It describes no real organisation, past or present.

What this sample shows

The pages that follow are the toolkit's own print-ready Board & CEO report (the Print_View tab), exactly as it prints after an organisation has answered the criteria. Nothing was edited by hand. The profile used:

- a public charitable trust working in education and health in three states, with about 45 staff;
- an online donor database, beneficiary records that include children, and two foreign donors;
- not a Significant Data Fiduciary.

What the buyer receives

Scope	Digital Personal Data Protection Act, 2023 and DPDP Rules, 2025
Core assessment	56 questions across 6 weighted pillars
NGO modules	45 optional questions: international donors and GDPR, social-sector field operations, Section 8 company / trust / society
Evidence base	505 Yes/No maturity criteria (Level 1 to Level 5); scores calculate automatically
Outputs	Board summary, 30/60/90-day plan, critical-gap flags, Board checklist, assurance report, action tracker, year-on-year trend
Format	One Excel workbook (16 sheets), single-organisation perpetual licence. Price: US$100

Key dates (as at 30 September 2026)

The DPDP Rules, 2025 were notified in November 2025 and apply in phases: Consent Manager provisions about 12 months after notification (November 2026), and most duties of data fiduciaries (notice, consent, security safeguards, breach notification and data principal rights) about 18 months after notification (May 2027). Check the current notifications before relying on any date.

Disclaimer

This report and the toolkit are self-assessment and gap-identification aids for educational and governance purposes. They are not legal advice, not an audit and not a compliance certification, and they do not generate privacy notices, consent forms or other legal documents. Scores reflect the answers entered. For decisions about your own organisation, take advice from a qualified professional. Check the current text of the Act, the Rules and any notifications before acting.

CA Sunil Kumar, FCA · sunilkumarfca.com · sunil@sunilkumarfca.com

DPDP Act Compliance Assessment

Board & CEO Report — Illustrative Sample (Fictional Organisation) — Self-assessment / gap identification only

Organisation	XYZ Foundation (fictional)
Entity Type	Public charitable trust (illustrative)
Assessment Period	FY 2026–27, Q2 (illustrative)
Prepared By	Grievance Officer (illustrative) (18-Sep-2026)
Approved By	Board of Trustees (illustrative) (30-Sep-2026)

2.93

Overall Core Compliance Maturity (out of 5.0): Level 3 – Defined

High Risk — Significant Gaps

2 Must-Have item(s) flagged as critical gaps (Level 1 or not assessed)

Gap to 4.0 floor: -1.07 | Benchmark: not entered

Core Pillar Scores

#	Pillar	Score	Maturity Level	Weight	Visual (0–5) | Risk Rating
P1	Governance, Accountability & Assurance	2.93	Level 3 – Defined	10%	■■■■■□□□□ High Risk — Significant Gaps
P2	Notice, Consent & Lawful Processing	2.96	Level 3 – Defined	20%	■■■■■□□□□ High Risk — Significant Gaps
P3	Data Principal Rights Management	3.17	Level 3 – Defined	15%	■■■■■□□□□ Elevated Risk — Below Regulatory Floor (4.0)
P4	Security Safeguards & Breach Management	2.76	Level 3 – Defined	25%	■■■■■□□□□ High Risk — Significant Gaps
P5	Third-Party, Cross-Border & SDF Obligations	3.10	Level 3 – Defined	15%	■■■■■□□□□ Elevated Risk — Below Regulatory Floor (4.0)
P6	Children, Vulnerable Groups & Regulatory Engagement	2.76	Level 3 – Defined	15%	■■■■■□□□□ High Risk — Significant Gaps
	OVERALL CORE SCORE (weighted)	**2.93**	**Level 3 – Defined**	100%	**High Risk — Significant Gaps**

Optional Module Overlays (informational — not in the core score)

M7	Module 7 — International Donors & GDPR Applicability	2.70	Level 3 – Defined	8 / 8 answered	■■■■■□□□□□
M8	Module 8 — Social Sector & Field Operations Governance	2.67	Level 3 – Defined	22 / 22 answered	■■■■■□□□□□
M9	Module 9 — Section 8 Company / Trust / Society Regulatory Intersection	3.16	Level 3 – Defined	10 / 15 answered	■■■■■■□□□□

Must-Have Items — Critical Gap Status

Q#	Question	Score	Final Level	Urgency	Status
Q2	DPO / Grievance Officer Appointment	3.40	Level 3 – Defined	Critical	**OK — above Level 1**
Q18	Notice Adequacy	3.40	Level 3 – Defined	Urgent	**OK — above Level 1**
Q19	Consent Capture Mechanism	3.40	Level 3 – Defined	Urgent	**OK — above Level 1**
Q21	Consent Withdrawal Handling	2.60	Level 3 – Defined	High	**OK — above Level 1**
Q23	Purpose Limitation	2.60	Level 3 – Defined	High	**OK — above Level 1**
Q24	Data Minimization	3.40	Level 3 – Defined	High	**OK — above Level 1**
Q26	Consent Document Adequacy	3.40	Level 3 – Defined	Urgent	**OK — above Level 1**
Q27	Right to Access	3.40	Level 3 – Defined	High	**OK — above Level 1**
Q28	Right to Correction & Erasure	3.40	Level 3 – Defined	High	**OK — above Level 1**
Q29	Grievance Redressal Mechanism	4.20	Level 4 – Managed	Urgent	**OK — above Level 1**
Q34	Technical Security Controls	4.20	Level 4 – Managed	High	**OK — above Level 1**
Q35	Organizational Security Controls	3.40	Level 3 – Defined	High	**OK — above Level 1**
Q37	Breach Notification — Data Protection Board	1.00	Level 1 – Vulnerable	Urgent	⚠ **CRITICAL GAP — Board attention required**
Q38	Breach Notification — Data Principals	1.80	Level 2 – Reactive	Urgent	**OK — above Level 1**
Q39	Data Retention Schedule	2.60	Level 3 – Defined	High	**OK — above Level 1**
Q40	Secure Disposal & Erasure	2.60	Level 3 – Defined	High	**OK — above Level 1**
Q44	Processor / Vendor / Partner / Staff Agreements	2.60	Level 3 – Defined	High	**OK — above Level 1**
Q46	Cross-Border Transfer Compliance	3.40	Level 3 – Defined	High	**OK — above Level 1**
Q52	Children's Data & Verifiable Parental Consent	1.00	Level 1 – Vulnerable	Urgent	⚠ **CRITICAL GAP — Board attention required**
Q55	DPB Engagement & Penalty Risk Readiness	2.60	Level 3 – Defined	High	**OK — above Level 1**

DPDP Act Compliance Assessment

Board & CEO Report — Illustrative Sample (Fictional Organisation) — Self-assessment / gap identification only

30 / 60 / 90 Day Action Plan & Executive Narrative

0–30 Days: IMMEDIATE

URGENT: 2 Must-Have item(s) are flagged ⚠️ CRITICAL GAP (list above). Name an owner for each in Action_Tracker, notify the Board, and start remediation now. No core pillar is at Level 1 (Vulnerable). Close every Critical-priority question first (Action_Tracker, Priority = Critical).

31–90 Days: SHORT-TERM

No core pillar is below Level 3. Close remaining Urgent and High-priority items and file evidence for each. 6 of 6 core pillars are currently below the 4.0 floor.

3–12 Months: MEDIUM-TERM

Move Level 3 pillars to Level 4 (Managed): monitoring, periodic Board reporting and evidence that controls operate. Lowest-scoring pillar to prioritise: Security Safeguards & Breach Management. Target an overall core score of at least 4.0 within 12 months, working toward 5.0; plan Medium/Planned-urgency items in the annual budget, complete applicable Modules 7–9, and log the re-assessment in YoY_Trend.

Executive Narrative

This assessment shows an overall core compliance maturity of 2.93 out of 5.0 (Level 3 – Defined), with 2 Must-Have item(s) flagged as critical gaps requiring immediate attention. Priority should go to closing Must-Have gaps in Pillar 4 (Security & Breach Management) and Pillar 6 (Children & Regulatory Engagement), which carry the highest statutory penalty exposure under the DPDP Act. This is a self-assessment output for gap identification and should inform, not replace, legal review of your compliance programme.

The action plan and narrative are maintained once (Board_Summary) so this page always reflects a single source of truth.

DPDP Act Compliance Assessment

Board & CEO Report — Illustrative Sample (Fictional Organisation) — Self-assessment / gap identification only

Question-Wise Assessment by Pillar and Module

Per-question score, status and recommended action. Status: Met ≥ 4.0 | Attention 3.0–3.99 | Critical < 3.0. For owners, dates and progress see Assurance_Report.

P1: Governance, Accountability & Assurance | Score: 2.93 | Level 3 – Defined

Q#	Question	Score	Status	Urgency / Applies to	Recommended Action
Q1	Board Oversight	3.40	Attention	Medium	Action: Add data protection as a standing item in Board/leadership meetings, with a nominated owner. | Gaps: 2 gap(s) — see column R.
Q2	DPO / Grievance Officer Appointment	3.40	Attention	Critical	Action: Appoint a named Grievance Officer, publish contact details on your website/notices, and define their authority in writing. | Gaps: 2 gap(s) — see column R.
Q3	Data Protection Policy Framework	3.40	Attention	Medium	Action: Draft a board-approved data protection policy covering notice, consent, security, retention, and grievance handling. | Gaps: 2 gap(s) — see column R.
Q4	Privacy Impact Assessment / DPIA Governance	2.60	Critical	Medium	Action: Create a simple DPIA template and require it before launching any new system or large data-collection activity. | Gaps: 3 gap(s) — see column R.
Q5	Cross-Functional Data Governance	2.60	Critical	Medium	Action: Set up a small cross-functional data protection working group that meets periodically. | Gaps: 3 gap(s) — see column R.
Q6	Training & Awareness	3.40	Attention	High	Action: Build a short induction module and an annual refresher session on data handling practices. | Gaps: 2 gap(s) — see column R.
Q7	Records of Processing Activities (ROPA)	1.80	Critical	High	Action: Build a simple spreadsheet/register listing each data category, purpose, source, storage location, retention period, and owner; review it every 6-12 months. | Gaps: 4 gap(s) — see column R.
Q8	Privacy by Design	2.60	Critical	Medium	Action: Add a privacy checklist/sign-off step to your project or system rollout process. | Gaps: 3 gap(s) — see column R.
Q9	Compliance Monitoring	2.60	Critical	Medium	Action: Schedule a half-yearly internal compliance review using this tool or a simplified checklist. | Gaps: 3 gap(s) — see column R.
Q10	Compliance Documentation & Evidence	2.60	Critical	High	Action: Create a single, organized folder (physical or cloud) where every compliance document is filed and version-dated. | Gaps: 3 gap(s) — see column R.
Q11	Privacy Reporting to Board	2.60	Critical	Medium	Action: Add a short data protection status update to periodic Board/management reporting. | Gaps: 3 gap(s) — see column R.
Q12	Data Classification	2.60	Critical	Medium	Action: Tag your ROPA entries as 'General', 'Sensitive', or 'Highly Sensitive' and apply stronger controls to the latter two. | Gaps: 3 gap(s) — see column R.
Q13	Exemptions Assessment	3.40	Attention	Medium	Action: List any processing relying on an exemption, note the legal basis, and review it annually. | Gaps: 2 gap(s) — see column R.
Q14	Regulatory Change Monitoring	4.20	Met	Medium	Action: Assign one person to check for DPDP Rules/notification updates quarterly and log any resulting policy changes. | Gaps: 1 gap(s) — see column R.
Q15	Compliance Responsibility Matrix	2.60	Critical	Planned	Action: Create a one-page RACI (Responsible/Accountable/Consulted/Informed) chart for key data protection tasks. | Gaps: 3 gap(s) — see column R.
Q16	Change Management	2.60	Critical	Medium	Action: Add a one-line privacy check to your existing change-approval process. | Gaps: 3 gap(s) — see column R.
Q17	Personal Data (PII) Definition	3.40	Attention	High	Action: Write a simple one-page list of what your organization treats as personal data, with examples, and share it with all staff. | Gaps: 2 gap(s) — see column R.

P2: Notice, Consent & Lawful Processing | Score: 2.96 | Level 3 – Defined

Q#	Question	Score	Status	Urgency / Applies to	Recommended Action
Q18	Notice Adequacy	3.40	Attention	Urgent	Action: Prepare notices in the languages your actual beneficiaries/donors speak, and always include withdrawal steps and grievance contact details. | Gaps: 2 gap(s) — see column R.
Q19	Consent Capture Mechanism	3.40	Attention	Urgent	Action: Switch from verbal-only consent to signed forms, logged digital consent, or recorded verbal consent with a timestamp. | Gaps: 2 gap(s) — see column R.
Q20	Consent Manager Readiness	2.60	Critical	Planned	Action: Check whether any partner platforms use Consent Managers and confirm your systems can interface with them; note Consent Manager registration under DPDP Rules 2025 opens November 2026. | Gaps: 3 gap(s) — see column R.
Q21	Consent Withdrawal Handling	2.60	Critical	High	Action: Provide a simple withdrawal channel (same channel as consent was given) and build a checklist to confirm processing stops. | Gaps: 3 gap(s) — see column R.
Q22	Legitimate Uses Assessment	3.40	Attention	Medium	Action: List any processing done without consent, and note which legitimate-use ground applies. | Gaps: 2 gap(s) — see column R.
Q23	Purpose Limitation	2.60	Critical	High	Action: Check current data uses against original notices; stop or re-notify/re-consent for any use beyond the original purpose. | Gaps: 3 gap(s) — see column R.
Q24	Data Minimization	3.40	Attention	High	Action: Review each data collection form and remove fields that aren't strictly necessary. | Gaps: 2 gap(s) — see column R.
Q25	Legacy Data Notice & Fresh Consent	1.80	Critical	Medium	Action: Identify pre-Act data, and run a notice/re-consent campaign for the categories that need it. | Gaps: 4 gap(s) — see column R.
Q26	Consent Document Adequacy	3.40	Attention	Urgent	Action: Update your consent form/process template to include all four elements: what, why, how long, and how to withdraw. | Gaps: 2 gap(s) — see column R.

P3: Data Principal Rights Management | Score: 3.17 | Level 3 – Defined

Q#	Question	Score	Status	Urgency / Applies to	Recommended Action
Q27	Right to Access	3.40	Attention	High	Action: Set up a simple internal process to pull together and share a person's data on request within a reasonable time. | Gaps: 2 gap(s) — see column R.
Q28	Right to Correction & Erasure	3.40	Attention	High	Action: Set an internal SLA (e.g., 15-30 days) for correction/erasure requests and track it. | Gaps: 2 gap(s) — see column R.
Q29	Grievance Redressal Mechanism	4.20	Met	Urgent	Action: Publish a simple grievance email/form with a committed response time, and track every complaint to closure. | Gaps: 1 gap(s) — see column R.
Q30	Right to Nominate	1.80	Critical	Medium	Action: Add a nomination field to your intake forms, and define what proof (death certificate, medical certificate) is needed to act on a nomination. | Gaps: 4 gap(s) — see column R.
Q31	Rights Request SLA Tracking	2.60	Critical	Medium	Action: Keep a simple log (spreadsheet is fine) of every rights request with date received and date resolved. | Gaps: 3 gap(s) — see column R.
Q32	Data Accuracy & Completeness	3.40	Attention	Medium	Action: Add a periodic 'data refresh' step for key records, especially before decisions or external sharing. | Gaps: 2 gap(s) — see column R.
Q33	Two-Tier Grievance Protocol	3.40	Attention	Medium	Action: State clearly in your grievance notice that internal resolution should be attempted first, with a defined internal timeline. | Gaps: 2 gap(s) — see column R.

P4: Security Safeguards & Breach Management | Score: 2.76 | Level 3 – Defined

Q#	Question	Score	Status	Urgency / Applies to	Recommended Action
Q34	Technical Security Controls	4.20	Met	High	Action: Implement basic encryption for sensitive data at rest/in transit, role-based access controls, and activity logging. | Gaps: 1 gap(s) — see column R.
Q35	Organizational Security Controls	3.40	Attention	High	Action: Document a security policy, schedule periodic access reviews, and add security clauses to vendor contracts. | Gaps: 2 gap(s) — see column R.
Q36	Breach Detection Capability	2.60	Critical	Medium	Action: Set up basic monitoring/alerts (even simple ones like login alerts) on systems holding personal data. | Gaps: 3 gap(s) — see column R.
Q37	Breach Notification — Data Protection Board	1.00	Critical	Urgent	Action: Write a one-page breach-notification procedure matching Rule 7's required content, naming who notifies the Board and how quickly after discovery. | Gaps: 5 gap(s) — see column R.
Q38	Breach Notification — Data Principals	1.80	Critical	Urgent	Action: Prepare a template Data-Principal breach notification in advance, matching Rule 7's required content, so it can go out within 72 hours of notifying the Board. | Gaps: 4 gap(s) — see column R.
Q39	Data Retention Schedule	2.60	Critical	High	Action: Add a retention period column to your ROPA for each data category, and check it against Rule 8's erasure framework (including any advance-notice-before-deletion steps if you run user accounts, e.g. a donor/member portal). | Gaps: 3 gap(s) — see column R.
Q40	Secure Disposal & Erasure	2.60	Critical	High	Action: Maintain a simple deletion log (what, when, who authorized) whenever data is purged. | Gaps: 3 gap(s) — see column R.
Q41	Breach Response Testing	1.80	Critical	Medium	Action: Run a simple tabletop exercise once a year — walk through a mock breach and note what worked and what didn't. | Gaps: 4 gap(s) — see column R.
Q42	Privileged Access Management	3.40	Attention	Medium	Action: Review who has admin/elevated access every 6 months, and remove access immediately when someone changes roles or leaves. | Gaps: 2 gap(s) — see column R.

DPDP Act Compliance Assessment

Board & CEO Report — Illustrative Sample (Fictional Organisation) — Self-assessment / gap identification only

Q43	Backup & Recovery	4.20	Met	Planned	Action: Encrypt backups, and test restoring from backup at least once a year. | Gaps: 1 gap(s) — see column R.

P5: Third-Party, Cross-Border & SDF Obligations | Score: 3.10 | Level 3 – Defined

Q#	Question	Score	Status	Urgency / Applies to	Recommended Action
Q44	Processor / Vendor / Partner / Staff Agreements	2.60	Critical	High	Action: Add a standard data protection/confidentiality clause to every vendor, partner, staff, and volunteer agreement template. | Gaps: 3 gap(s) — see column R.
Q45	Third-Party Due Diligence	2.60	Critical	Medium	Action: Add a short pre-engagement privacy/security questionnaire for any new vendor handling personal data. | Gaps: 3 gap(s) — see column R.
Q46	Cross-Border Transfer Compliance	3.40	Attention	High	Action: Before any new cross-border data flow, check it against the current government-notified restriction list. | Gaps: 2 gap(s) — see column R.
Q47	SDF Classification Monitoring	4.20	Met	Medium	Action: Review SDF classification criteria annually against your data volumes and processing activities. | Gaps: 1 gap(s) — see column R.
Q48	DPIA for Significant Data Fiduciaries	3.40	Attention	Medium	Action: If classified as an SDF, schedule and document a DPIA at the required interval. | Gaps: 2 gap(s) — see column R.
Q49	Independent Data Audit	3.40	Attention	Medium	Action: If classified as an SDF, engage an independent auditor annually and act on findings. | Gaps: 2 gap(s) — see column R.
Q50	AI, Profiling & Automated Decision-Making Governance	2.60	Critical	Planned	Action: Add a privacy review step before adopting any AI tool or automated decision system that touches personal data. | Gaps: 3 gap(s) — see column R.
Q51	Data Sharing Register	2.60	Critical	Medium	Action: Keep a simple log of every external data share: what, why, legal basis, and who received it. | Gaps: 3 gap(s) — see column R.

P6: Children, Vulnerable Groups & Regulatory Engagement | Score: 2.76 | Level 3 – Defined

Q#	Question	Score	Status	Urgency / Applies to	Recommended Action
Q52	Children's Data & Verifiable Parental Consent	1.00	Critical	Urgent	Action: Add an age-check step to any beneficiary intake involving minors, and obtain and record verifiable parental/guardian consent. | Gaps: 5 gap(s) — see column R.
Q53	Tracking/Targeted Advertising Restriction	4.20	Met	Medium	Action: Turn off behavioural tracking/ad personalization on any platform or page aimed at children. | Gaps: 1 gap(s) — see column R.
Q54	Persons with Disabilities — Guardian Consent	2.60	Critical	Medium	Action: Check whether any beneficiaries have a legal guardian on record, and route consent through them where applicable. | Gaps: 3 gap(s) — see column R.
Q55	DPB Engagement & Penalty Risk Readiness	2.60	Critical	High	Action: Designate who handles DPB communication, and keep your compliance evidence folder ready to produce on request. | Gaps: 3 gap(s) — see column R.
Q56	Appellate Escalation (TDSAT)	3.40	Attention	Planned	Action: Identify legal counsel familiar with TDSAT appeals in advance, so the organization isn't scrambling if an order needs to be challenged. | Gaps: 2 gap(s) — see column R.

M7: Module 7 — International Donors & GDPR Applicability | Score: 2.70 | Level 3 – Defined

Q#	Question	Score	Status	Urgency / Applies to	Recommended Action
M7-1	Grant Agreement DPA/SCC Alignment	3.40	Attention	Overlay	Action: Request or draft a DPA/SCC template for every foreign grant agreement, clarifying controller/processor roles up front. | Gaps: 2 gap(s) — see column R.
M7-2	Cross-Border Transfer Risk Assessment	2.60	Critical	Overlay	Action: Run a simple transfer risk check (what data, why, how protected) before sending data abroad, and use encryption for sensitive files. | Gaps: 3 gap(s) — see column R.
M7-3	Legitimate Interest Assessment (LIA)	2.60	Critical	Overlay	Action: Write a short LIA note (purpose, necessity, balancing test) whenever M&E reporting relies on legitimate interest instead of consent. | Gaps: 3 gap(s) — see column R.
M7-4	Special Category Data Protections	3.40	Attention	Overlay	Action: Flag any health/religious/political data fields in your ROPA and add an explicit consent or public-interest justification step. | Gaps: 2 gap(s) — see column R.
M7-5	Joint Controllership in Collaborative Research	2.60	Critical	Overlay	Action: Add a data governance and rights-handling clause to research/consortium partnership agreements. | Gaps: 3 gap(s) — see column R.
M7-6	FCRA-DPDP-GDPR Reporting Overlap	2.60	Critical	Overlay	Action: Review donor/FCRA report templates and redact or aggregate beneficiary data wherever individual-level detail isn't required. | Gaps: 3 gap(s) — see column R.
M7-7	Beneficiary Media & Testimonial Consent	1.80	Critical	Overlay	Action: Use a simple signed media-consent form before publishing any beneficiary photo, video, or testimonial. | Gaps: 4 gap(s) — see column R.
M7-8	International Breach Escalation (GDPR 72-Hour)	2.60	Critical	Overlay	Action: Add the donor and any GDPR 72-hour requirement to your breach-notification procedure alongside the DPDP Board notification step. | Gaps: 3 gap(s) — see column R.

M8: Module 8 — Social Sector & Field Operations Governance | Score: 2.67 | Level 3 – Defined

Q#	Question	Score	Status	Urgency / Applies to	Recommended Action
M8-1	Beneficiary Data Classification	2.60	Critical	Overlay	Action: Tag beneficiary records as 'general' or 'sensitive' in your programme database, and apply stronger access controls to the latter. | Gaps: 3 gap(s) — see column R.
M8-2	Minimum Necessary Beneficiary Data	3.40	Attention	Overlay	Action: For each programme, write a short list of exactly which beneficiary fields are collected and why, and remove any that aren't strictly needed. | Gaps: 2 gap(s) — see column R.
M8-3	Beneficiary Data Accuracy Review	2.60	Critical	Overlay	Action: Schedule a periodic (e.g., annual) data-refresh review of active beneficiary records. | Gaps: 3 gap(s) — see column R.
M8-4	Beneficiary Consent	1.80	Critical	Overlay	Action: Use a simple consent step at intake for any sensitive data collection or planned use of photos/testimonials. | Gaps: 4 gap(s) — see column R.
M8-5	M&E/Survey Data Protection	2.60	Critical	Overlay	Action: Apply the same access controls and encryption standards to survey/M&E datasets as to core programme data. | Gaps: 3 gap(s) — see column R.
M8-6	Research Data Anonymization	3.40	Attention	Overlay	Action: Strip or mask direct identifiers (name, phone, ID numbers) from datasets before sharing them for research or reporting. | Gaps: 2 gap(s) — see column R.
M8-7	Donor Privacy Requirements Identification	3.40	Attention	Overlay	Action: Keep a one-page summary of each major donor's specific privacy/data requirements, alongside the grant file. | Gaps: 2 gap(s) — see column R.
M8-8	Donor Agreement Privacy Review	2.60	Critical	Overlay	Action: Add a privacy-clause check to your standard donor-agreement review/sign-off process. | Gaps: 3 gap(s) — see column R.
M8-9	Donor Reporting System Compliance	3.40	Attention	Overlay	Action: Include donor reporting/CRM systems in your regular security and privacy review cycle. | Gaps: 2 gap(s) — see column R.
M8-10	Partner Due Diligence	2.60	Critical	Overlay	Action: Use a short privacy/security checklist before onboarding any new implementing partner who will handle personal data. | Gaps: 3 gap(s) — see column R.
M8-11	Partner Data-Sharing Documentation	1.80	Critical	Overlay	Action: Add a simple data-sharing clause (what's shared, why, safeguards, breach reporting) to every partner MOU/agreement. | Gaps: 4 gap(s) — see column R.
M8-12	Partner Privacy Practice Review	2.60	Critical	Overlay	Action: Re-check key partners' privacy practices annually, especially those handling sensitive beneficiary data. | Gaps: 3 gap(s) — see column R.
M8-13	Field Device (BYOD) Security	1.80	Critical	Overlay	Action: Require passcodes and enable remote-wipe on any device (organizational or personal) used to collect beneficiary data. | Gaps: 4 gap(s) — see column R.
M8-14	Offline Data Collection & Sync	2.60	Critical	Overlay	Action: Set a rule to upload and securely delete/shred offline data within a defined short window after collection. | Gaps: 3 gap(s) — see column R.
M8-15	Paper Record Physical Safeguards	3.40	Attention	Overlay	Action: Store sensitive paper records in a locked cabinet with access limited to named staff. | Gaps: 2 gap(s) — see column R.
M8-16	Offline Sync & Remote Wipe	1.80	Critical	Overlay	Action: Enable remote-wipe/device-management features on organizational tablets and phones used in the field. | Gaps: 4 gap(s) — see column R.
M8-17	Need-to-Know Access	2.60	Critical	Overlay	Action: Set up role-based access so field staff only see the records for their own assigned area/cases. | Gaps: 3 gap(s) — see column R.
M8-18	Offboarding Access Revocation	3.40	Attention	Overlay	Action: Add access-revocation as a mandatory step on your staff/volunteer/intern offboarding checklist. | Gaps: 2 gap(s) — see column R.
M8-19	Staff/Volunteer Confidentiality Clauses	3.40	Attention	Overlay	Action: Add a standard confidentiality/data-protection clause to every employment, volunteer, and consultant agreement template. | Gaps: 2 gap(s) — see column R.
M8-20	SaaS/Cloud Tool Vetting	2.60	Critical	Overlay	Action: Turn on 2FA and review privacy/sharing settings for every SaaS tool that touches personal data. | Gaps: 3 gap(s) — see column R.
M8-21	AI Tool Usage Guidance	1.80	Critical	Overlay	Action: Write a one-page AI usage guidance note: what staff can and can't paste into AI tools, and circulate it to all staff. | Gaps: 4 gap(s) — see column R.
M8-22	AI Prohibition & Human Review	2.60	Critical	Overlay	Action: Make it a clear rule: no confidential personal data into unauthorized AI tools, and human review of any AI output involving personal data before use. | Gaps: 3 gap(s) — see column R.

M9: Module 9 — Section 8 Company / Trust / Society Regulatory Intersection | Score: 3.16 | Level 3 – Defined

DPDP Act Compliance Assessment

Board & CEO Report — Illustrative Sample (Fictional Organisation) — Self-assessment / gap identification only

Q#	Question	Score	Status	Urgency / Applies to	Recommended Action
M9-1	Legal Structure & Applicable Regime Mapping	3.40	Attention	All Entities	Action: Note your entity type in your ROPA header and list the specific filings (MCA, Charity Commissioner, or Registrar of Societies) that involve personal data. | Gaps: 2 gap(s) — see column R.
M9-2	Governing Body Personal Data	2.60	Critical	All Entities	Action: Add governing-body member files to your ROPA and apply the same access restrictions as other sensitive records. | Gaps: 3 gap(s) — see column R.
M9-3	Director/KMP Data via MCA21	—	Not Assessed	Section 8 Company	Not yet assessed — answer criteria in Criteria_Input, or enter a manual score in column F.
M9-4	Statutory Registers & Board Minutes	—	Not Assessed	Section 8 Company	Not yet assessed — answer criteria in Criteria_Input, or enter a manual score in column F.
M9-5	Related Party Transaction (RPT) Register	—	Not Assessed	Section 8 Company	Not yet assessed — answer criteria in Criteria_Input, or enter a manual score in column F.
M9-6	CSR-1/CSR-2 Beneficiary Data Flows	3.40	Attention	All Entities (if CSR-1 registered)	Action: Before sending beneficiary data for CSR reporting, check whether aggregated/anonymized figures would satisfy the donor's disclosure needs instead of individual-level data. | Gaps: 2 gap(s) — see column R.
M9-7	Trustee Data & Public Trust Filings	3.40	Attention	Trust	Action: Document who prepares and files trustee data with the Charity Commissioner, and store copies of filings securely. | Gaps: 2 gap(s) — see column R.
M9-8	Trust Deed Amendments & Trustee Changes	3.40	Attention	Trust	Action: Create a simple checklist for trustee changes: update internal records, notify the Charity Commissioner, and securely archive the outgoing trustee's data per your retention schedule. | Gaps: 2 gap(s) — see column R.
M9-9	Managing Committee & Member Data / Registrar Filings	—	Not Assessed	Society	Not yet assessed — answer criteria in Criteria_Input, or enter a manual score in column F.
M9-10	Bye-Law Amendments & Membership Records	—	Not Assessed	Society	Not yet assessed — answer criteria in Criteria_Input, or enter a manual score in column F.
M9-11	12A/80G Registration Data Sharing	4.20	Met	All Entities	Action: Apply the same access controls to 12A/80G filing data as to other sensitive financial-personal data, and share only what the filing requires. | Gaps: 1 gap(s) — see column R.
M9-12	Aadhaar Handling for Beneficiary Verification	2.60	Critical	All Entities	Action: Collect masked Aadhaar (last 4 digits) wherever the full number isn't specifically required, and check your Aadhaar storage practices against current UIDAI circulars. | Gaps: 3 gap(s) — see column R.
M9-13	Auditor & Regulatory Filing Data Sharing	2.60	Critical	All Entities	Action: Prepare data extracts for auditors/regulators with only the fields actually required, and confirm confidentiality obligations are in the audit engagement letter. | Gaps: 3 gap(s) — see column R.
M9-14	Whistleblower / Vigil Mechanism Data	3.40	Attention	All Entities	Action: Restrict vigil-mechanism case files to a small named group, and store them separately from general HR records. | Gaps: 2 gap(s) — see column R.
M9-15	Regulatory Enforcement Timeline Readiness	2.60	Critical	All Entities	Action: Build your compliance plan against the earlier possible date, and assign someone to monitor official gazette notifications for any acceleration. | Gaps: 3 gap(s) — see column R.