ManageEngine
IT Security

5

tactical wins that move

DPDP

Act compliance

from theory to practice

Introduction

The 90-day
roadmap for digital trust

The Digital Personal Data Protection Act (DPDP Act) isn't just a legal requirement. It's a chance to rethink how your organization handles security and data governance. For CISOs, it's a unique opportunity to turn compliance into meaningful, measurable progress that reduces risk within the first 90 days.

This playbook is built for senior data protection leaders that want a clear, practical path to accelerate compliance, boost audit readiness, and earn lasting trust across the organization. It also helps CISOs gather the right evidence and shape a compelling story that shows how DPDP Act compliance can strengthen governance, build investor confidence, and ultimately enhance market value.

Key objectives

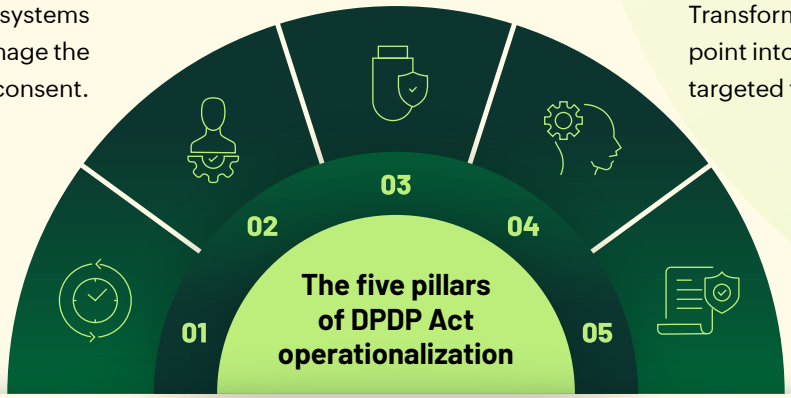
Automated consent logging
Engineer automated systems to prove, track, and manage the full lineage of consent.

Shadow IT discovery
Gain a complete, real-time view of data flows across all environments.

Tag high-risk data flows
Build a risk-aware data fabric where sensitivity automatically drives protection.

Engineer sustainable behavior change
Transform the workforce from a risk point into a human firewall through targeted training.

Pilot a DPIA-as-code framework
Institutionalize data protection impact assessments (DPIAs) directly into development pipelines.



In this guide, we will share five non-negotiable objectives to help you move beyond paper policies and institutionalize compliance:

Impact metrics: What success looks like

After the 90 days of implementing these objectives, you can measure the success of this implementation by the following metrics:

Shadow data exposure

Measures the reduction in the volume of unmonitored or unauthorized systems, applications, or integrations that access, process, or store personal data without formal governance.

Consent integrity

Represents the percentage of personal data records that have valid, purpose-specific, time-bound, and verifiable consent from the data principal, as required by the DPDP Act.

DPIA automation

Tracks the implementation and coverage of DPIAs for high-risk data processing activities.

Workforce readiness

Assesses the percentage of employees who have completed and demonstrated proficiency in role-based data protection and privacy awareness training aligned with the DPDP Act.

OBJECTIVE 1

Shadow IT discovery

Turn the unknown into quantifiable risk

Goal: Expose, quantify, and control hidden data flows and unauthorized, high-risk tools that create immediate regulatory exposure.

WEEKS 1–2

Comprehensive asset scan

Execute a cloud access security broker (CASB) scan across unmanaged SaaS and API traffic. Leverage discovery tools to generate a complete inventory of SaaS and IaaS assets. Cross-reference network logs with procurement and billing records to identify shadow tools purchased directly by business units.

WEEKS 3–4

Data egress mapping

Analyze firewall and proxy logs to identify systems actively transmitting data to external IPs or unregistered third-party clouds without official authorization.

WEEKS 5–6

Risk classification and ownership

Classify high-risk applications based on the sensitivity of data processed and compliance gaps. Assign and document clear ownership in the configuration management database.

WEEKS 7–8

Containment and remediation

Make sure any tools that haven't been approved are either removed or isolated in a secure testing environment. For critical applications, ask vendors to promptly sign data processing agreements that meet DPDP Act compliance standards.

WEEKS 9–12

Automate continuous monitoring

Integrate CASB feeds directly into your SIEM platform (or choose a SIEM with a built-in CASB functionality like ManageEngine Log360) to continuously flag and alert on new unsanctioned tools.

Go further:

Pair shadow IT discovery with shadow data mapping

Look beyond rogue SaaS usage to uncover where personal data actually travels, which APIs it touches, what storage systems it lands in, and whether it leaves your jurisdiction. Use the correlation from CASB, SIEM, and endpoint telemetry to trace the flow and destination of data, not just the tool processing it.

For example, your marketing team might use an approved CRM like Salesforce, and Zoho CRM but SIEM logs could reveal that exported lead lists, containing phone numbers and Aadhaar-linked data, are being synced through a third-party email automation tool hosted overseas. The CRM is compliant, but the data journey isn't. By combining CASB discovery with data flow telemetry, you can detect that cross-border transfer in near-real time, classify it as a policy violation, and automatically quarantine or block the unapproved integration.

What to do now:

- Update and share clear guidelines on how tools should be used and how new vendors get onboarded.
- Establish a simple, mandatory process for registering any new SaaS tools before they're used.
- Set up ongoing alerts to flag any unapproved tools, and make sure those alerts go straight to the privacy team for quick review.

OBJECTIVE 2

Automated consent logging

Build legal defensible evidence, not just records

Goal: Prove you can clearly trace how and when user consent was given so there's a full record of it. Uphold the rights of every individual whose data you handle. Establish systems in place that make compliance airtight and easy to audit.

WEEKS 1–2

Define the consent schema

Collaborate with legal and application teams to define a schema that captures the user ID, processing purpose, and a precise timestamp.

WEEKS 3–4

Deploy a consent API gateway

Set up one central service that collects and manages all user consents from every application in the same way.

WEEKS 5–6

Integrate with identity systems

Ensure every consent record is mapped to a verified user identity to establish absolute traceability.

WEEKS 7–9

Implement immutable storage

Keep consent records in tamper-proof storage, like a write once read many system or blockchain, so they're always verifiable.

WEEKS 10–12

Automate revocation triggers

When consent is withdrawn, automatically revoke processing privileges across relevant systems via an IAM solution (like ManageEngine AD360) and data catalogs.

Go further:

Treat consent like important data, not just an on/off switch. Store each consent action in a secure log that can't be altered, with a digital signature to prove when and how it was given.

What to do now:

- Select a reliable consent management solution, whether open-source, commercial or even a custom-built API.
- Integrate consent APIs with your CRM and data lakes to ensure policies are enforced directly at the data layer.
- Develop real-time dashboards that clearly display active, expired, and withdrawn consents for full visibility and control.

OBJECTIVE 3

Tag high-risk data flows

Make sensitivity actionable

Goal: Create a smart data system that automatically checks how sensitive data is as soon as it's collected. Based on that sensitivity, it should instantly apply the right protection policies to keep the data safe.

WEEKS 1–3

Automated personal information classification

Begin by finding where personal and sensitive data resides across your organization.

Deploy automated discovery tools such as Log360 with DataSecurity Plus to scan on-premises and cloud environments for identifiers like Aadhaar, PAN, financial, or health data.

This phase focuses on detection and classification, building a clear inventory of what types of personal data you hold, where it lives, and who owns it.

WEEKS 4–6

Define risk taxonomy

Design your sensitivity labeling system—a simple, consistent way to categorize data by risk and sensitivity.

Decide on short, readable tags such as SENSITIVE_FIN, EMPLOYEE_HEALTH, or PUBLIC_PII.

Collaborate with the legal team to ensure these categories align with the DPDP Act's definitions of personal and special data, and with business units to make sure the taxonomy reflects how data is actually used across HR, finance, and customer support.

WEEKS 7–8

Apply tags across schemas

With the taxonomy finalized, move from design to implementation.

Apply the defined tags directly to databases, data lakes, and pipelines, so each table, column, or record carries its sensitivity label (e.g., SENSITIVE_FIN or EMPLOYEE_HEALTH).

Use your data catalog to trace how tagged data flows—where it starts, where it moves, and who interacts with it.

By embedding labels within your systems, sensitive data becomes machine-readable and trackable, enabling automation in the next phase.

WEEKS 9–10

Automate enforcement rules

Tie access control and data retention rules directly to each sensitivity tag so that protection happens automatically, not manually.

For example, data tagged SENSITIVE_FIN can automatically require MFA, encryption, and shorter retention periods, while data tagged PUBLIC_PII can follow more flexible rules.

WEEKS 11–12

Continuous reclassification

Schedule automated, periodic scans to detect and correct any untagged or misclassified data.

Go further:

Enforce policy-driven tagging at ingestion points
Use attribute-based access control (ABAC) to automatically connect your DLP policies and access rules to each data tag. ABAC lets you make access decisions based on data attributes like sensitivity tags and user attributes like role, department, or location.

What to do now:

- Update the governance charter to clearly define ownership and accountability for each data tag category.
- Implement DLP and cloud policies that automatically trigger alerts and blocks upon tag violations.
- Schedule monthly privacy reviews to proactively manage tag drift and exception handling.

OBJECTIVE 4

Engineer sustainable behavior change

Turn cyber vigilance into muscle memory

Goal: Transform employees from the biggest risk point into an active human firewall and a frontline defense against data incidents.

WEEKS 1–3

Launch role-based micro-modules

Provide tailored privacy training modules designed specifically for different teams like HR, DevOps, and marketing so each group understands how privacy applies to their unique roles and responsibilities.

WEEKS 4–6

Departmental gamified challenges

Create realistic data scenarios and challenges that reflect each department's daily workflow, helping teams practice and reinforce the right responses.

WEEKS 7–9

Simulated incident drills

Conduct company-wide mock consent leak and data mishandling drills to practice DPDP Act breach notification procedures and technical response.

WEEKS 10–12

Behavior-based scoring rollout

Create a scoring dashboard that shows how better employee behavior leads to fewer real incidents. Track things like training completion, reporting of suspicious activity, and policy violations, then compare these scores with actual data incidents.

Example:
If your HR and finance teams score higher on privacy awareness this quarter, and their number of accidental data leaks drops by 40%, the dashboard shows that training is working.

Go further:

Measure response behavior, not just completion
Track how many employees proactively flag suspicious data behavior like phishing, unusual data access versus simply finishing a module.

What to do now:

- se learning management platforms that feature adaptive testing to focus on weak spots.
- Conduct tabletop exercises with legal and HR to practice the DPDP Act's stringent breach notification timelines.
- Link training scores and proactive behavior metrics to annual performance appraisals for accountability.

OBJECTIVE 5

Pilot a DPIA-as-code framework

Operationalize privacy by design

Goal: Turn the DPIA from a one-time checklist into a dynamic, automated system that continuously monitors and assesses data risks throughout the life cycle of your projects.

WEEKS 1–2

Select high-risk pilot process

Find a new or recently changed data process that handles a lot of personal data or sensitive information; something that could have a big privacy impact if not managed properly.

Example:
A new customer profiling system that combines purchase history, location, and demographics to personalize offers—this kind of process should be reviewed first because it uses large amounts of sensitive customer data.

WEEKS 3–5

Auto-map data flows

Automatically map and visualize how data moves through your systems by using the metadata already stored in your data catalog tools.

These tools can show you where data starts, where it travels, and which systems or users access it, without having to manually trace every connection.

WEEKS 6–8

Quantify privacy risk

Create simple scripts or tools that calculate privacy risk using a standard scoring model, like Likelihood × Impact. This helps you measure how serious each risk is and prioritize what needs attention first.

Then build dashboards to visualize these scores, so you can quickly see which processes or systems carry the highest privacy risk.

WEEKS 9–10

Integrate DPIA trigger into CI/CD

Implement a lightweight API call or script that automatically triggers a DPIA whenever a new data asset or API is added to a CI/CD pipeline.

WEEKS 11–12

Validate and formalize

Test your automation process to make sure it works correctly across different systems, then fine-tune the risk scoring so it reflects real-world privacy risks. Once it's reliable, turn it into a standard template that every team in the organization can use.

Example:
After piloting your automated DPIA workflow, adjust the scoring so high-volume marketing data gets higher risk weight than internal HR data. Then roll out the final version as the official DPIA model for all new projects.

Go further:

Think of the DPIA as an automatic checkpoint, not a one-time project. Set up your systems so that whenever a new feature, API, or data process is deployed, the DPIA runs automatically before it goes live. This ensures every change involving personal data is reviewed for privacy risks—and compliance can't be skipped or forgotten.

What to do now:

- Develop reusable DPIA templates that are directly aligned with DPDP Act Sections 8–11.
- Build risk quantification scripts that automatically flag high-risk components and non-compliant processing.
- Build dashboards to track DPIA completion status, residual risk levels, and mitigation progress.

Next on your roadmap:

The first 90 days lays the groundwork—establishing core policies, mapping data flows, and launching foundational controls. After the 90-day foundational setup, you are ready to move beyond checkboxes and build a privacy program that holds up under scrutiny, stress, and scale. It should focus on high-risk obligations that carry significant penalties, emerging technologies like AI, and the operational realities of cross-border data movement.

Phase	Initiative	What to do	Why it matters
Months 1–3 Solidify core processes and high-risk controls	Adversarial breach response testing	Engage an external red team to simulate a targeted data breach. Test detection, containment, legal response, and crisis communication.	Internal drills are useful, but real-world simulations reveal hidden weaknesses and build team confidence.
	Data governance framework for minors	Audit systems for minor data. Implement parental consent mechanisms and block tracking or profiling of children.	Children's data is highly protected under the DPDP Act. Mishandling it risks severe penalties and reputational damage.
Months 4–6 Address advanced obligations and future risks	Prepare for Significant Data Fiduciary (SDF) status	Assess if your organization qualifies as an SDF. Appoint a resident DPO and schedule independent audits.	SDF designation brings stricter oversight. Early preparation ensures smoother compliance and audit readiness.
	Cross-border data transfer framework	Map all outbound data flows. Identify destination countries, legal bases, and update vendor contracts for DPDP Act compliance.	Enables compliant global operations and prevents unauthorized transfers that could trigger enforcement actions.
	AI and ML model governance policy	Audit models for consent-based training data. Prevent reverse engineering and support data correction or deletion requests.	AI systems pose unique privacy risks. This policy ensures innovation aligns with DPDP Act obligations.

The goal? Turn every compliance effort into proof of **stability, efficiency,** and **ethical leadership.**

Stability

Efficiency

Ethical leadership

The three indicators investors and regulators reward most:

1. Institutionalize a regulatory resilience program to prove you're penalty-proof.

Goal:

Position the company as regulation-proof, visibly less likely to face fines or compliance incidents.

Why it impacts stock value:

Markets reward stability. When a company can prove that it's resilient to regulatory risk, investors factor in lower future uncertainty, which boosts valuation and investor confidence.

How to do it:

- Build a regulatory readiness dashboard that tracks and reports DPDP Act compliance KPIs monthly. Include consent accuracy, DPIA coverage, breach response time, vendor compliance rate, etc.
- Publish key highlights internally and in quarterly investor briefings. For example, *Zero DPDP Act violations in 12 months or Vendor compliance score: 98%.*
- Run yearly mock audits to help teams prepare for real regulatory checks and highlight areas where they're improving.

2. Create a trust transparency report to turn privacy into brand equity.

Goal:

Use privacy transparency as a competitive differentiator that strengthens reputation and customer loyalty.

Why it impacts stock value:

When companies handle data transparently and responsibly, they earn trust from customers, investors, and partners alike. That trust strengthens the brand and fuels long-term growth in both revenue and market value.

How to do it:

- Issue a semiannual trust transparency report summarizing how your organization protects data. Include metrics like adherence to data retention guidelines, consent withdrawal fulfillment rates, and a non-sale of personal data policy.
- Include simple visuals and plain-language summaries—no jargon, just clear proof of integrity.
- Align it with environmental, social, and governance (ESG) reporting, since data ethics increasingly fall under the governance pillar.

3. Operationalize compliance efficiency to show that compliance saves money.

Goal:

Prove to the board that strong compliance doesn't just avoid penalties—it reduces operational cost and increases margins.

Why it impacts stock value:

Efficiency drives profitability and smart investors take notice. Companies that stay compliant while using fewer resources demonstrate strong operational discipline and governance maturity, all key indicators in ESG performance.

How to do it:

- Lay out your key compliance activities, like DPIA reviews, consent audits, and vendor assessments. Then track how much time and money each one takes. It's a smart way to spot inefficiencies and improve how your team works.
- After 6–9 months, present your findings to the board: *We reduced compliance cycle time by 40% and external audit prep costs by ₹X crore.*
- In investor communications, tie these savings directly to earnings before interest, taxes, depreciation, and amortization gains to highlight operational efficiency and governance maturity.

Related solutions

ManageEngine AD360

ManageEngine AD360 is a unified IAM solution securing digital identities with adaptive MFA and role-based access control. It prevents insider threats, while ensuring compliance and minimizing unauthorized access risks.

To learn more,

Sign up for a personalized demo

ManageEngine Log360

ManageEngine Log360 is a unified SIEM platform combining UEBA, DLP, CASB, and SOAR to detect threats, protect networks, monitor the dark web, and automate response. It enables faster incident resolution, reducing breach impact and compliance risk.

To learn more,

Sign up for a personalized demo