SOC2TIX-AR

DPDPA Compliance Advisory to Secure India's Most Consequential Data Governance Era

A strategic briefing for leadership teams to navigate extraterritorial mandates, consent-first frameworks, and the path to defensible readiness.

CREST Registered Region - Global

VA PEN TEST

certin Empanelled

The Gaps Most Organizations Don't See

Penalties reach up to INR 250 Crore (~$30M) for failure to implement reasonable security safeguards.
-Section 33, DPDPA

Dimensions of India's New Data Reality

Extraterritorial

Applies to any entity worldwide processing Indian citizen data.

850M+ Users

India represents one of the world's largest consumer data pools.

No Small Biz Carve-Out

Obligations apply to ALL Data Fiduciaries regardless of size.

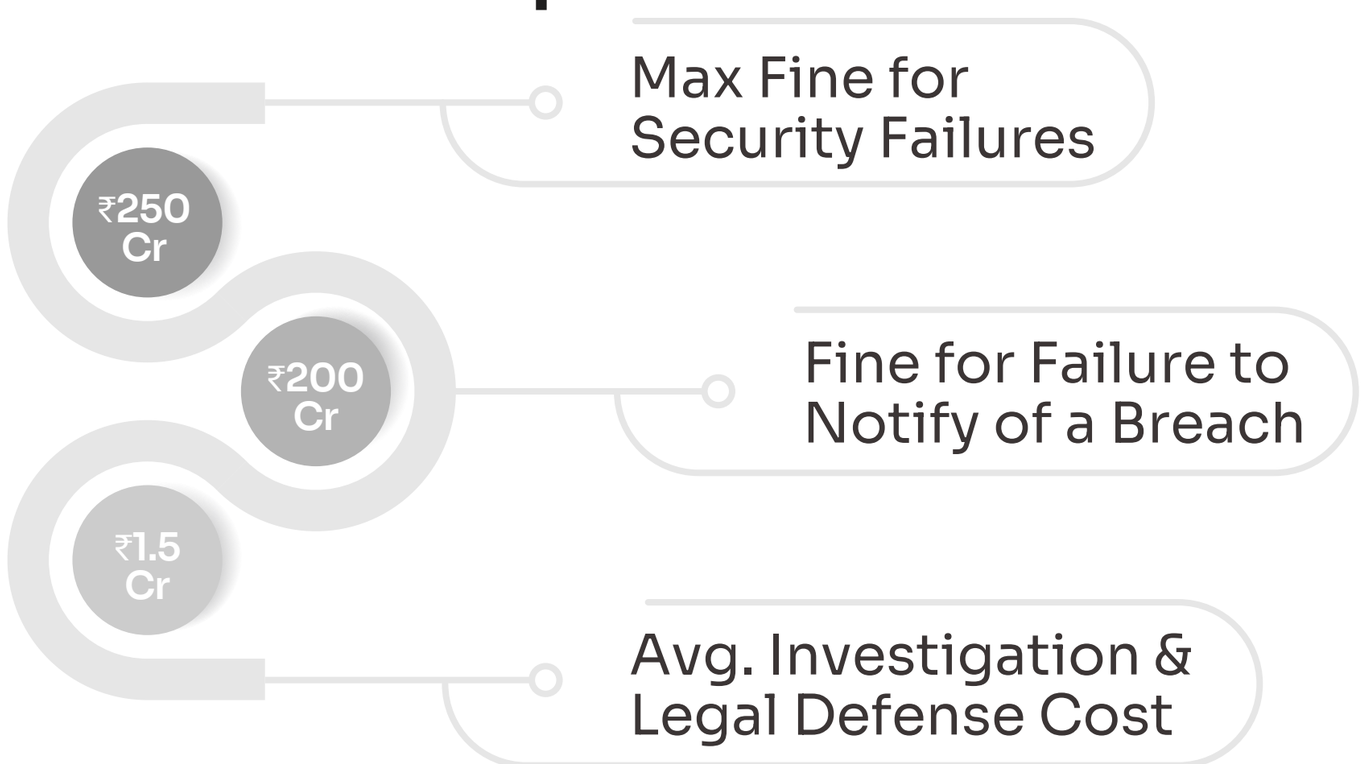
Top 5 Risk

India ranks in the Top 5 globally for data breach volume.

What You Think vs What We Find

Common Belief	Technical/Legal Reality
We are GDPR compliant, so we are safe.	DPDPA has no "legitimate interest" basis for commercial data, consent is primary.
We have time until enforcement begins	Gaps built now create liability that cannot be cleared retroactively.
Existing privacy notices are sufficient	DPDPA requires multilingual accessibility and specific prescribed content.

The Real Cost of Inaction — Why Prevention Is 30—60x Cheaper



Actual ROI

Your Actual ROI Calculation

INR 15 Lakhs to 1 Crore

Up to INR 250 Crore per violation

Enterprise clients now mandate DPDPA compliance for all vendors

Common Resistance We Hear

What Clients Say	Why It Costs More	The Fact
Our sector localization is enough	DPDPA transfer rules are distinct from RBI/SEBI mandates	Localization does not equal DPDPA compliance
We use policy templates	Policy doesn't fix a lack of "Withdrawal UX" or Consent Managers	DPDPA requires verifiable withdrawal capability

What We Test

Active Vulnerabilities in Your Environment

Identity & Consent

Lack of verifiable "Withdrawal of Consent" mechanisms across all touchpoints.

Data Flow

Unmapped cross-border transfers to nondesignated (blacklisted) jurisdictions.

Access Rights

Inability to fulfill Data Principal requests for Erasure or Portability within timelines.

Data Quality

Processing inaccurate or outdated personal data in violation of Section 8.

Shadow Data

Indian citizen data stored in unencrypted environments without security safeguards.

Vendor Risk

Processing agreements (DPAs) that lack DPDPA-specific liability clauses.

Did You Know? Under DPDPA, failure to notify the Data Protection Board (DPB) of a breach can result in a separate penalty of up to INR 200 Crore.

Our Assessment Scope

Every Layer, Every Component

Consent Management

- Multilingual Privacy Notices
- Unambiguous Opt-in Logic
- Withdrawal Ease-of-Use

Data Fiduciary Obligations

- Storage Limitation Audits
- Data Processor Contract Review
- Grievance Redressal Mechanisms

Data Principal Rights

- Access/Correction Workflows
- Right to Nominate Review
- Erasure/Portability Readiness

Significant Data Fiduciary (SDF)

- India-based DPO Appointment
- Data Protection Impact Assessment
- Independent Data Auditor Review

Technical Safeguards

- CREST-Approved VAPT
- ISO 27001 Alignment
- Incident Response Calibration

Cross-Border Transfers

- Transfer Whitelist Mapping
- Contractual Safeguards
- Data Flow Visualization

Our Methodology

What Happens at Every Step

Each phase is designed to build on the last, from discovery through to continuous compliance, ensuring no gap is left unaddressed across your entire data governance posture.

Your Decision

Who Manages Your Data Risk First?

Without DPDPA Program

- Legacy GDPR notices lack DPDPA format.
- Unmapped cross-border liability.
- No DPB-ready breach workflow.
- Board carries growing liability.

With Briskinfosec Program

- Multilingual, prescribed-format notices.
- Full flow mapping against whitelist.
- Calibrated IR plan with DPB templates.
- Evidence-based readiness reporting.

What We Need to Start

Privacy Policies and Notices

Access to current Privacy Policies and Notices.

Data Inventory ROPA

Data inventory/records of processing activities (ROPA).

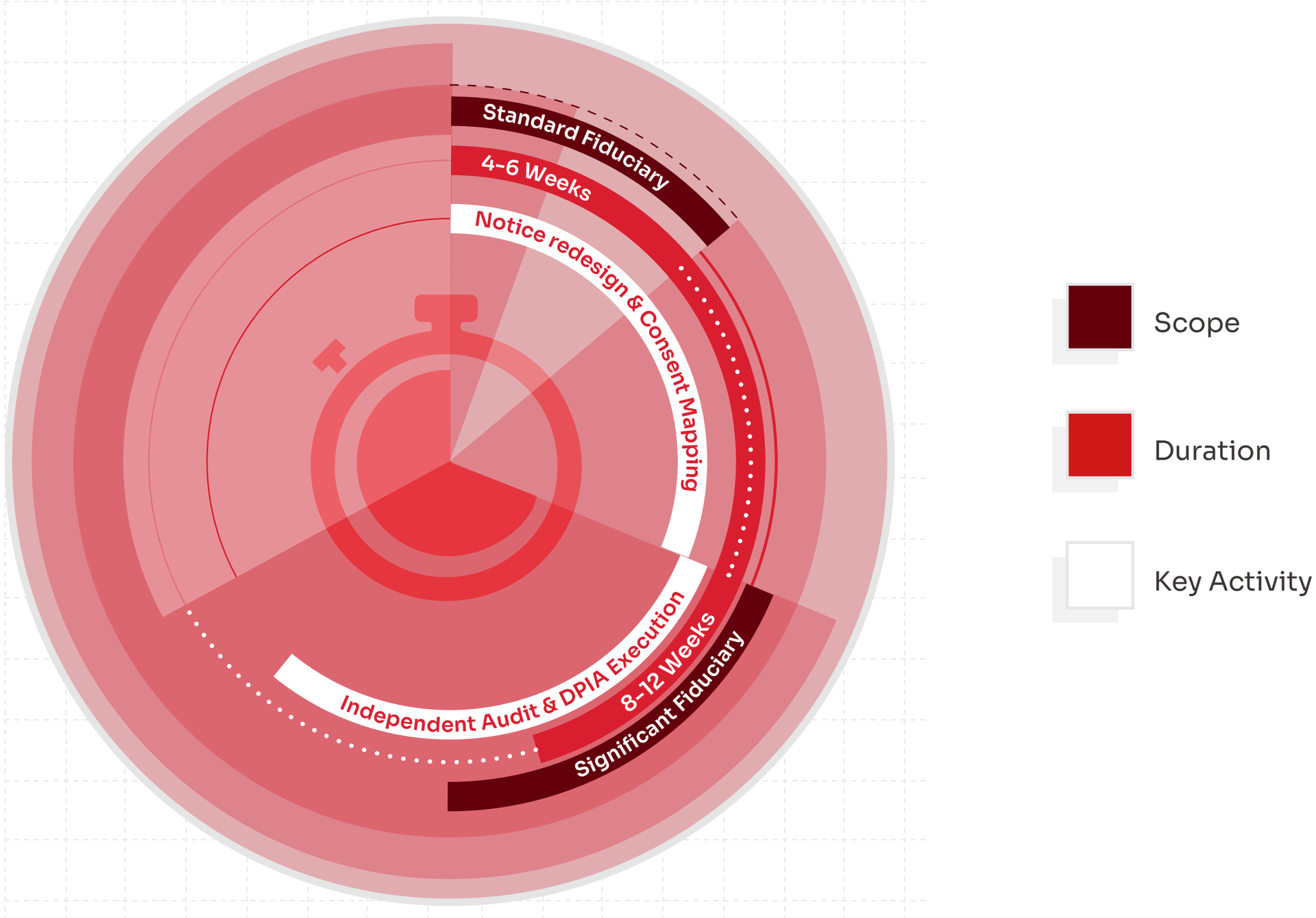
3rd-Party Processors

List of 3rd-party Data Processors and current contracts.

IR & Grievance Procedures

Current Incident Response and Grievance procedures.

Timeline Drivers



Client Breaches
Post-assessment security record

Start With Zero Commitment

Understanding your unique security challenges begins with a conversation. We offer a no-obligation consultation to assess your current posture and identify immediate risk areas.

Our Team Holds Industry-Leading Certifications

We invest heavily in our team's continuous education because the threat landscape never stops evolving. Neither do we.

OSCP | OSWE | CISSP | CISA | CEH

CREST Accredited
Internationally certified penetration testing excellence

CERT-IN Empanelled
Government-recognized trusted cybersecurity assessment provider

ISO 27001 : 2022 Certified
Our own security practices are independently audited and verified annually

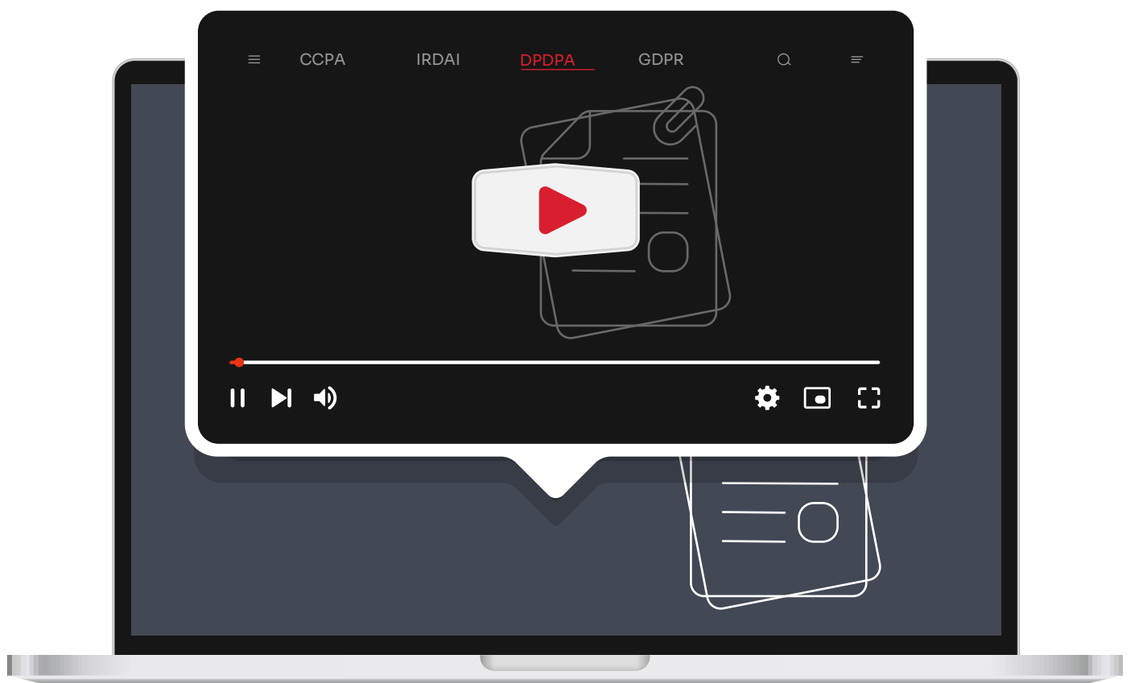
25+
Countries Client Portfolio

67%
Logic flaws missed by bots

98%
Client retention

640+
Successful Customers

5600+
Delivered in 24 countries



Reach us for FREE
consultation

Book Now

sales@briskinfosec.com
www.briskinfosec.com

Our Geographical Presence India UAE