Vendor Privacy Assessment

Prepared by Cipher Guardians

A structured framework for evaluating privacy and operational risks across third-party systems and vendors.

Vendor Discovery

Identify all vendors receiving, processing, storing, or analyzing customer and employee information.

Operational Risk Review

Review exports, retention policies, access governance, subprocessors, and monitoring practices.

Contract & Governance

Assess contractual visibility, escalation workflows, operational accountability, and periodic reassessment practices.

High-Risk Categories

Analytics platforms, CRM systems, cloud providers, marketing tools, support systems, and workforce platforms often require deeper review.

Review Area	Focus
Governance	Ownership, workflows, accountability
Consent	Collection, propagation, withdrawal

Engineering	Masking, retention, minimization
Analytics	Dashboard exposure, warehouse governance
Monitoring	Audit logs, exports, downstream visibility

Operational Implementation Considerations

Organizations should operationalize privacy governance beyond documentation. This includes embedding controls into onboarding workflows, ETL pipelines, warehouses, dashboards, analytical systems, reporting environments, and downstream integrations.

Need help operationalizing privacy governance?

Cipher Guardians helps organizations improve DPDP readiness, privacy engineering maturity, analytics governance, consent management, and operational privacy workflows.

Book a consultation:
https://thecipherguardians.com