BRISKDATA ENGINEERING TEMPLATE | DOC ID: BD-ENG-PRR-006 | ADAPTABLE TEMPLATE

Production Readiness Review (PRR) Checklist

7-Gate Go/No-Go Review Across Identity, Data, Webhooks, Secrets, Observability, Capacity, and Rollback

HOW TO RUN THIS 7-GATE REVIEW

Complete this 21-item checklist (three verification items across each of the seven launch gates) 5 to 10 business days before launching a new service, major release, inherited application, or AI-assisted codebase. Link objective evidence for each applicable item and record any time-bounded risk acceptances in Section 8.

Gate 1: Identity, Tenant Isolation, and Least-Privilege Access

- [ ] **Server-Side Tenant Scoping:** Every read, write, export, and background job enforces tenant/organization ownership server-side (verified with negative cross-tenant tests).
- [ ] **Scoped Workload Permissions:** Runtime compute uses least-privilege IAM roles and network rules rather than wildcard admin credentials or static keys in source files.
- [ ] **Protected Administrative Routes:** Internal admin and support-impersonation endpoints enforce MFA, restricted access, and immutable audit logging.

Gate 2: Data Durability, Backups, and Restore Timing

- [ ] **Continuous Point-in-Time Recovery:** Automated snapshots and continuous transaction-log archival (PITR) are enabled with retention aligned to business RPO.
- [ ] **Timed Isolated Restore Test:** At least one full backup restore into an isolated environment has been executed, verified for integrity, and timed against target RTO.
- [ ] **Safe Schema Migration Pipeline:** Database migrations enforce explicit lock timeouts and follow backward-compatible expand/contract deployments.

Gate 3: Webhook Idempotency and External Dependency Timeouts

- [ ] **Inbound Webhook Verification:** Payment and third-party webhooks verify raw-body cryptographic signatures, replay windows, and unique event-ID idempotency keys.
- [ ] **Outbound Mutation Idempotency:** External payment charges, ledger posts, and fulfillment calls send deterministic idempotency keys to prevent duplicate execution on retry.
- [ ] **Bounded Client Timeouts & Retries:** Every outbound HTTP, database, SMTP, and AI/LLM client sets explicit connect/read timeouts and bounded retries with backoff.

Gate 4: Secrets Hygiene, Rotation, TLS, and DNS Readiness

- [ ] **Clean Repository History:** Secret scanning across full Git history confirms zero committed API keys, database URLs, or private signing keys.
- [ ] **Zero-Downtime Key Rotation:** Signing secrets, API tokens, and database credentials reside in a managed vault and support rotation without forced downtime.
- [ ] **TLS Auto-Renewal & Cutover TTLs:** Certificate renewal validation is verified and cutover DNS records have TTL lowered 24 to 48 hours ahead of launch.

Gate 5: SLIs, Actionable Alerting, and Redacted Logging

- [ ] **User-Facing SLIs Defined:** Availability, latency (p95/p99), and async queue-age indicators are instrumented on core customer and billing paths.
- [ ] **Symptom-Based Paging:** High-urgency alerts trigger on user-visible error burn or synthetic check failure and link directly to an operational runbook.

- [ ] **PII & Secret Log Redaction:** Structured logs include request/trace IDs while redacting passwords, bearer tokens, payment data, SSNs, and raw secrets.

Gate 6: Connection Pooling, Query Plans, and Rate Ceilings

- [ ] **Database Connection Pooling:** Autoscaled/serverless compute connects through a transaction pooler (such as PgBouncer or RDS Proxy) sized within database limits.
- [ ] **Production-Scale Query Plans:** Launch-critical queries and indexes have been checked with EXPLAIN ANALYZE against representative data volumes.
- [ ] **Abuse & Spend Rate Limits:** Per-IP and per-tenant rate limits and budget caps protect authentication, export, search, and AI inference endpoints.

Gate 7: Tested Rollback and Operational Ownership

- [ ] **Rehearsed Backout Plan:** Prior artifact rollback and post-change verification steps (BD-OPS-BKO-004) have been executed and timed in staging.
- [ ] **Live On-Call Alert Test:** Primary and secondary responders have received a test page and verified emergency production access.
- [ ] **Account & Vendor Ownership Recorded:** Domain, cloud billing, monitoring, and third-party vendor accounts are registered under company control.

8. Go / No-Go Sign-Off and Exception Log

Rate any deferred exception using Likelihood (1-5) x Impact (1-5): 15-25 Critical, 10-14 High, 5-9 Moderate, 1-4 Low. Unmitigated Critical or High items require explicit executive deferral or written temporary risk acceptance.

Reviewer Role	Name	Decision	Evidence / Exception Expiry	Date
Application / Tech Lead	[Name]	[ ] GO [ ] CONDITIONAL [ ] DEFER	[PRR Ticket / Link]	YYYY-MM-DD
Infrastructure / SRE	[Name]	[ ] GO [ ] CONDITIONAL [ ] DEFER	[Restore & Pooler Proof]	YYYY-MM-DD
Security Reviewer	[Name]	[ ] GO [ ] CONDITIONAL [ ] DEFER	[AuthZ & Secret Scan]	YYYY-MM-DD
Business / Product Owner	[Name]	[ ] GO [ ] CONDITIONAL [ ] DEFER	[Accepted Risk & Date]	YYYY-MM-DD

Template Reuse Note: You may copy and adapt this template for internal operations within your organization. Replace bracketed placeholders and remove example entries before adoption. briskData branding and third-party trademarks remain the property of their respective owners.