BRISKDATA ENGINEERING TEMPLATE | DOC ID: BD-ENG-TRN-007 | ADAPTABLE TEMPLATE

Software Transition and Application Handoff Checklist

Account Ownership, Architecture Discovery, Clean-Room Builds, Shadow Operations, and Acceptance

OWNERSHIP AND OPERATIONAL RESPONSIBILITY

Keep legal and billing ownership distinct from day-to-day operational support. Domain registrars, cloud management accounts, source repositories, payment processors, and signing certificates belong in accounts owned by the client organization, with delegated administrative access granted to the incoming support team. Pair this checklist with the 30-item Software Transition Handoff Tracker (.xlsx / .csv).

1. Example Four-Phase Transition Schedule (Adapt to Overlap Window)

Phase	Example Window	Primary Objectives	Verification Gate
Phase 1: Continuity & Account Control	Days 1 - 5	Freeze destructive changes; verify company ownership of domains, DNS, cloud root/billing, Git orgs, and emergency contacts.	Client-owned root accounts & MFA verified.
Phase 2: Architecture & Clean Build	Days 6 - 12	Map services, data stores, integrations, and cron jobs; build and deploy staging from controlled source without personal laptops.	Clean-room staging build succeeds.
Phase 3: Shadow Operations	Days 13 - 22	Incoming team executes a supervised release, acknowledges test alerts, and restores representative backup data in isolation.	Release, alert path, and restore verified.
Phase 4: Acceptance & Revocation	Days 23 - 30	Document open risks, rotate shared secrets/API keys, revoke outgoing contractor access, and sign transition acceptance.	Secrets rotated; acceptance signed.

2. Six-Workstream Handoff Verification Checklist

- [ ] **1. Ownership & Access:** Domain registrar, authoritative DNS, cloud billing/root, Git organization, package/container registries, and mobile signing accounts confirmed under client ownership.
- [ ] **2. Architecture & Data:** Current topology diagram, runtime/dependency support matrix, regulated data map, scheduled jobs, and known defects documented.
- [ ] **3. Build, Release & Recovery:** CI/CD pipeline, deployment steps, rollback procedure, monitoring alerts, and isolated database backup restore tested by the incoming team.
- [ ] **4. Product & Support Knowledge:** Critical business workflows, recurring support tickets, maintenance windows, and SLA commitments reviewed with business owners.
- [ ] **5. Vendor & Integration Transfer:** Payment gateways, transactional email/SMS (SPF/DKIM/DMARC), SSO/OAuth apps, and support contracts updated to authorized client contacts.
- [ ] **6. Access Revocation & Secret Rotation:** Outgoing SSH keys, IAM users, VPN profiles, personal access tokens, and shared webhook/database secrets rotated or revoked after verifying dependencies.

3. Transition Acceptance and Open-Risk Sign-Off

Record any inherited technical debt or security findings using Likelihood (1-5) x Impact (1-5): 15-25 Critical, 10-14 High, 5-9 Moderate, 1-4 Low.

Role	Name & Organization	Disposition	Signature & Date
Client Business / System Owner	[Name / Client Org]	[ ] Accepted [ ] Conditional	_____ YYYY-MM-DD
Incoming Engineering Lead	[Name / Incoming Team]	[ ] Verified [ ] Exceptions Logged	_____ YYYY-MM-DD
Outgoing Technical Contact	[Name / Outgoing Team]	[ ] Handoff Delivered	_____ 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.