Technical Due Diligence Checklist – Company B

This document outlines the comprehensive technical due diligence requirements Company B applies during mergers and acquisitions. All target organizations must align with these standards prior to full integration to ensure compatibility, security, compliance, and operational efficiency.

1. Infrastructure Requirements

- All infrastructure should be defined as code (IaC) and stored in a version-controlled repository.
- Cloud resources should follow naming conventions, tagging, and be aligned with regional compliance requirements.
- Infrastructure must support horizontal scalability and high availability for production systems.

2. Data Management Standards

- Data encryption must be enforced at rest and in transit using AES-256 or stronger.
- Data storage and retention policies must comply with GDPR and CCPA guidelines.
- Data lineage and audit trails should be trackable via automated pipelines.
- PII and sensitive data must be classified and handled per ISO/IEC 27001 policies.

3. Application Architecture Alignment

- Microservices should be containerized (preferably with Docker) and orchestrated using Kubernetes.
- All services must expose REST or gRPC APIs with versioning and health checks.
- Legacy monoliths must have a documented roadmap for refactoring or modularization.

4. DevSecOps Practices

- CI/CD pipelines must include automated security scans, static analysis, and dependency checks.
- Credentials and API keys must be stored in secure vaults, not hard-coded in source code.
- Audit logs of deployments, rollbacks, and approvals must be maintained.

5. Logging, Monitoring, and Observability

- All production services should emit logs in structured JSON format and integrate with centralized logging systems (e.g., ELK, Datadog).
- Monitoring tools must track system uptime, error rates, CPU/memory usage, and alert on threshold breaches.
- Tracing (e.g., OpenTelemetry) should be in place to correlate service-to-service calls.

6. Software Quality Metrics

- Minimum 80% unit test coverage on all critical services.
- Regression testing must be automated and executed on every major commit.
- Code must comply with PEP8 (Python) or relevant linting rules and pass pre-merge checks.

7. Security Compliance and Certification

- Organization must demonstrate alignment with ISO/IEC 27001, SOC 2 Type II, and GDPR standards.
- Security policies should be reviewed quarterly and updated based on threat intelligence.
- Third-party penetration tests should be conducted at least annually, with tracked remediation plans.

8. Intellectual Property and Documentation

- All source code must have clear license ownership and contributor agreements.
- Architectural decisions should be documented using ADRs (Architecture Decision Records).
- Developer onboarding guides, API documentation, and system architecture diagrams must be up to date.