Risk Assessment

Compliance & Security Risks

1. No automated security scanning exposes system to vulnerabilities.
2. Inconsistent environments increase risk of misconfigured security groups, IAM roles, and secrets.
3. Manual database migrations risk data loss and non-compliance with audit requirements.
4. Lack of centralized monitoring makes it impossible to detect breaches quickly.
5. No traceability of deployments creates accountability gaps.

Stabilization Risks

1. Introducing IaC may cause temporary misconfigurations.
2. Database migration automation could still cause downtime if rollback is not validated.
3. Resistance from teams used to ad-hoc deployment methods.
4. CI/CD standardization may break existing manual workflows initially.
5. Short-term velocity drop as team adapts to changes.

Risk Minimization Processes

1. Introduce mandatory peer-review for all deployment pipelines.
2. Implement canary deployments before full rollout.
3. Automate backups before every migration.
4. Enforce security scanning (Snyk, Trivy, OWASP ZAP) in CI/CD pipeline.
5. Provide phased adoption with parallel manual fallback options during transition.
6. Assign incident response roles with defined escalation paths.