d) Risks in the propose Architecture

1. Availability & Deadline

Risk:
- Batch fails or runs past 09:00 SGT deadline.
- Single scheduler node failure stops orchestration.

Mitigation:
- Deploy scheduler/runner in HA (redundant nodes, leader election).
- Implement checkpointing + resumable jobs.
- Synthetic checks at 08:30 SGT and SNMP traps if SLA threatened.

2. Performance

Risk:
- Daily recompute (5,000 + 10n trades) exceeds 60-minute window.
- Portal cannot sustain 50 concurrent users with ≤3s internet latency.

Mitigation:
- Partition calculation by counterparty; parallel processing.
- Precompute aggregates for reuse within a run.
- Load-test portal with 50+ concurrent sessions; tune DB queries and caching.

3. Scalability

Risk:
- Growth to ~23k trades after 5 years leads to unacceptable run times.
- Adding more counterparties (20k+) causes DB bottlenecks.

Mitigation:
- Design engine to scale horizontally (add compute nodes).
- Archive raw inputs in object storage; partition staging DB.
- Capacity tests yearly; provision headroom (≥2× projected peak).

4. Security

Risk:
- Unauthorized access to reports or parameter changes.
- Data leakage outside internal bank network.

Mitigation:
- Enforce AuthN/AuthZ via RBAC: org-report role, counterparty role, param-editor roles.
- MFA + VPN required.
- Encrypt inputs/outputs at rest; TLS for all transport.
- Full audit log of parameter changes and report downloads.

5. Auditability / Traceability

Risk:
- Inability to reproduce old report (missing inputs or param version).
- Audit logs incomplete or tampered.

Mitigation:
- Store inputs and params ≥1 year in WORM storage.
- Every report stamped with param version + input set hash.
- Digitally sign audit logs and artifacts.

6. Operability & Monitoring

Risk:
- Fatal errors undetected until business users complain.
- SNMP traps fail to trigger monitoring.

Mitigation:
- Structured logs with severity levels; central log aggregation.
- SNMP trap redundancy; also publish alerts to message bus.
- Synthetic probe checks report availability at 08:30 SGT.

7. Configurability

Risk:
- Parameter changes not triggering recalculation.
- Overwrites old results, losing history.

Mitigation:
- Version parameters; parameter change always triggers full recalculation.
- Keep prior results tied to old parameter versions.
- Restrict param editing to audited roles.

8. Adaptability (RDS migration in 3 months)

Risk:
- Schema drift between current RDS and new RDS breaks ingestion.
- Tight coupling delays migration.

Mitigation:
- Implement anti-corruption layer / adapter for RDS.
- Use schema versioning + contract tests.
- Feature flag for dual-run and gradual switch-over.

9. Recoverability

Risk:
- Disk failure or data corruption causes loss of staging or reports.
- Disaster recovery not meeting RTO/RPO.

Mitigation:
- Daily cross-region backups; immutable object storage.
- Periodic DR drills; RTO ≤ 10h, rerun batch in ≤30 min after transient error.

10. Usability

Risk:

- Users confused by multiple report versions (different param sets).
- Complex UI slows adoption.

Mitigation:
- Clear labeling in portal (date, param version, status).
- Provide both CSV and XLSX outputs.
- Keep portal simple, English-only, role-based menus.