b) Scenarios

Performance:
- The deadline for the risk report is at 9.AM Singapore time, equivalent to 9.PM in New York and 2.AM in London.
- The batch job to calculate counterparty risk begins at 8:00 AM Singapore time and must complete within one hour. The 8:00 AM start is the baseline for running the daily batch.
- On the first run, the system calculates the risk report for approximately 5,000 trades. Each subsequent day, the batch job processes new trades generated that day (estimated at about 10 trades per day) and updates the counterparty risk results accordingly.

Scalability:
- Each day, the system recalculates risk for the organization and for each counterparty based on the full set of current data. The expected data size includes approximately 5,000 initial trades plus 10 × n new trades (after n days) across about 20,000 counterparties.
- The system must be able to efficiently identify which data has changed and which remains unchanged, so that recalculation is applied only where needed and previously computed, unchanged results can be reused.

Security:
- The system must enforce authentication (to verify user identity) and authorization (to control user access) before any reports can be accessed.
- Role-based access control (RBAC) must be implemented:
  - Users with an individual counterparty role may access reports related only to that counterparty.
  - Users with an organization role may access the overall organizational risk report.
- Separate roles must be defined for modifying risk calculation parameters:
  - One role may update parameters for organization-level calculations.
  - Another role may update parameters for counterparty-level calculations.
- Reports must only be accessible from within the bank’s internal global network (on-premises or secure VPN).

Availability:
- System acceptable downtime is less than 30 minutes/day. The availability is 98%

Adaptability:
- When the new Reference Data System is ready. The Financial Risk System must be configured to work with new system within 3 months. That is the time the legacy system to be decommissionized.

Configurability:
- The system must allow risk calculation parameters (e.g., thresholds, factors, stress multipliers) to be changed without modifying the application code.
- When parameters change, the system must recalculate all organizational and counterparty risks using the new values.
- Previous calculations must be retained and associated with the version of parameters used, ensuring traceability and reproducibility.
- Access to parameter modification must be role-based and logged for audit.

Auditability:
- The following events must be recorded in the system audit logs:
  - Report generation.
  - Modification of risk calculation parameters.

Traceability:
- The system should take appropriate steps to recover from an error if possible, but all errors should be logged.
- A Simple Network Management Protocol (SNMP) trap should be sent to the bank’s Central Monitoring Service in the

following circumstances:
  - When there is a fatal error with a system component.
  - When reports have not been generated before 9am Singapore time.