Financial Risk System

1. Context

A global investment bank based in London, New York and Singapore trades (buys and sells) financial products with other banks (“counterparties"). When share prices on the stock markets move up or down, the bank either makes money or loses it. At the end of the working day, the bank needs to gain a view of how much risk of losing money they are exposed to, by running some calculations on the data held about their trades. The bank has an existing Trade Data System (TDS) and Reference Data System (RDS) but needs a new Risk System.

1.1. Trade Data System

The Trade Data System maintains a store of all trades made by the bank. It is already configured to generate a file-based XML export of trade data to a network share at the close of business at 5pm in New York. The export includes the following information for every trade made by the bank:

- Trade ID, Date, Current trade value in US dollars, Counterparty ID

1.2. Reference Data System

The Reference Data System stores all of the reference data needed by the bank. This includes information about counterparties (other banks). A file-based XML export is also generated to a network share at 5pm in New York, and it includes some basic information about each counterparty. A new reference data system is due for completion in the next 3 months, and the current system will eventually be decommissioned. The current data export includes:

- Counterparty ID, Name, Address, etc...

2. Functional Requirements

1. Import trade data from the Trade Data System.
2. Import counterparty data from the Reference Data System.
3. Join the two sets of data together, enriching the trade data with information about the counterparty.
4. For each counterparty, calculate the risk that the bank is exposed to.
5. Generate a report that can be imported into Microsoft Excel containing the risk figures for all counterparties known by the bank.
6. Distribute the report to the business users before the start of the next trading day (9am) in Singapore.
7. Provide a way for a subset of the business users to configure and maintain the external parameters used by the risk calculations.

3. Non-functional Requirements

a. Performance

- Risk reports must be generated before 9am the following business day in Singapore.

b. Scalability

- The system must be able to cope with trade volumes for the next 5 years.
  - The Trade Data System export includes approximately 5000 trades now and it is anticipated that there will be slow but steady growth of 10 additional trades per day.
  - The Reference Data System export includes approximately 20,000 counterparties and growth will be negligible.
- There are 40-50 business users around the world that need access to the report.

c. Availability

- Risk reports should be available to users 24x7, but a small amount of downtime (less than 30 minutes per day) can be tolerated.

d. Failover

- Manual failover is sufficient, provided that the availability targets can be met.

e. Security

- This system must follow bank policy that states system access is restricted to authenticated and authorised users only.
- Reports must only be distributed to authorised users.
- Only a subset of the authorised users are permitted to modify the parameters used in the risk calculations.
- Although desirable, there are no single sign-on requirements (e.g. integration with Active Directory, LDAP, etc).
- All access to the system and reports will be within the confines of the bank's global network.

f. Audit

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

g. Fault Tolerance and Resilience

- The system should take appropriate steps to recover from an error if possible, but all errors should be logged.
- Errors preventing a counterparty risk calculation being completed should be logged and the process should continue.

h. Internationalization and Localization

- All user interfaces and reports will be presented in English only.
- All trading values and risk figures will be presented in US dollars only.

i. Monitoring and Management

- 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 the system.
  - When reports have not been generated before 9am Singapore time.

j. Data Retention and Archiving

- Input files used in the risk calculation process must be retained for 1 year.

k. Interoperability

- Interfaces with existing data systems should conform to and use existing data formats.

Frequently asked questions

- **What do you mean by the word "counterparty"?** Another bank that we do business with.
- **How fast are the risk calculations?** Assume that you can run all calculations, for all trades (5 years from now) in sequence, in less than one hour.
- **What's the output of the risk calculation?** The output is a risk score; a number between 1 and 100, determining how risky doing more business with another bank is.
- **What are the "parameters" that can be configured?** The parameters are just the constants used in the risk calculation algorithm. Let's say there are <10 numbers that can be changed.
- **Does the solution need to be on-premises, or can we use the cloud?** Your choice.
- **Which cloud provider does the bank use?** Your choice.
- **Does the bank have a standard set of technologies (e.g. programming languages, databases, etc)?** Your choice; make any assumptions you like.
- **Can we ask the TDS and RDS system owners to provide an API interface?** No, you must use their existing XML exports.
- **How do we get the XML export?** Let's assume that the TDS and RDS place the XML files on a network share that you own.
- **Should we send the risk reports to users, or should they download them from our software system?** Your choice.
- **Can we distribute the reports by uploading them to a content/documentation management system?** Your choice.
- **Are all users in the same country/office?** No, but any person in any country/office will be able to access the solution you are building, via the bank's network infrastructure.
- **Should we implement authentication ourselves, or can we use the bank's existing solution?** Your choice. Feel free to assume the bank has an existing Active Directory/LDAP/SSO solution that you can integrate with, and add groups to if needed.
- **Should we implement logging, auditing, and archiving systems ourselves, or can we use the bank's existing solutions?** Your choice, feel free to assume these exist.