Group 18 Risk Management Report

Technical and Managerial Risks

Technical	Priority
Failure of correct network architecture implementation	HIGH
Database Product	HIGH
Cannot provide accurate backups/logs	HIGH
Unable to provide intrusion detection solutions	MEDIUM
Failure to assign proper virus protection	LOW
Cannot meet system responses	LOW
Managerial	Priority
Inability to suitably manage the overall project	LOW
Inability to staff key positions	HIGH
Inadequate communication among team members	MEDIUM
Budget or schedule constraints	LOW
● Design not scalable	LOW
● Unavailable test facilities or resources	LOW

Risk Evaluation
(Most urgent to least urgent)

Risk	Probability	Risk (1-10)	Risk Exposure
Failure of correct network architecture implementation	60%	8	4.8
Database Product does not meet requirements	50%	7	3.5
Cannot provide accurate backups/logs	10%	6	0.6
Unable to provide intrusion detection solutions	10%	5	0.5
Failure to assign proper virus protection	10%	3	0.3
Cannot meet system responses	10%	2	0.2

1a. A risk response for failure of correct network architecture implementation is to **buy information** on it. In order to minimize this risk, we can simulate the network architecture on the packet tracer application to test that everything is working correctly.

1b. Another risk response is to **mitigate** the risk of network architecture failure. In order to mitigate the risk effectively, the company could hire a team of network engineers to look at the architecture. Give advice and directions on how to properly implement the architecture. That way the network engineering team will be able to mitigate the risks.

2a. A job of our team is to write requirements and specifications for a database product for the real estate company to use. A risk is after the database software is written, it's expensive to maintain that software. Perhaps one way to lessen the risk (**mitigate**) is to choose an API (Rets.ly, RETS, Zillow, etc) that is more future-proof.

2b. A risk that could be encountered when delivering the software product is a security loophole within the code. If provided software contained security issues, for example, as a result of tampered data, this risk would then be **accepted**. In turn, the contingency plan would be to throttle more on testing security measures of the code in the application, along with rigorous tests to ensure data is being processed in the software properly. Consulting for better security implementation might also be necessary. Loading previous, safe backups of the system.