Executive Summary for the Beta Development Project

A risk management assessment and a risk mitigation plan for the software infrastructure of the Beta Development Project will be performed. The project is currently under development. The proper security controls will need to be established before the go-live date.

For this project, over 100 developers are working in a LAN environment composed of a cluster of 80 Linux and Solaris servers (some with Oracle databases) and workstations. The Network File System (NFS) is configured on the servers and used as a distributed file system with working home directories for the developers. The developers are primarily using Micro Focus Application Lifecycle Management (ALM) for their project development work. The LAN also includes a web server and an email server. For non-IT work that needs to be performed, a Microsoft environment is used consisting of a Windows domain for HR and Finance authentication and servers running Microsoft SQL Server.

The following security vulnerabilities have been noted in the company's IT infrastructure:

- The Linux , Solaris and Windows administrators have database access that poses a security risk. For example, they are able to view the company's finances.
- The developers have database access in the production environment indicating that the development and production environments are not properly.
- The NFS file system is not secure and can easily be compromised.
- There are unauthorized code changes in the ALM.
- There are no reliable backup and disaster plans established.
- Password policies do not enforce complex passwords.
- In case of employee turnover, especially developers leaving the project, account lockout policies are not configured in the operating system (Linux and Solaris) and database systems.

To address the security vulnerabilities, the risk management team has recommended that least privilege access be enforced for HR and Finance. In addition, to properly separate the development and production environments on ALM, least privilege access should be enforced for administrators in the Unix like operating systems, Windows and Databases (Oracle and SQL Server). Netapp which is integrated with AWS should be used as a backup and disaster recovery solution. Alternatively, Splunk can be used for disaster recovery and backups. Lastly, NFS should be secured by configuring permissions and Kerberos.