**Exercise 3. Design Highly Available and Secure Architecture**

**Name: \_\_\_\_\_\_\_\_\_\_Zou Xuan\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_2019-02-17\_\_\_\_\_\_\_\_\_\_\_\_\_**

1. **Risk Assessment**

|  |  |  |
| --- | --- | --- |
| **Asset/Asset**  **Group** | **Potential Threat/Vulnerability**  **pair** | **Possible Mitigation Controls** |
| Web Application and DB Servers | There is no catering for availability of the services leading to Single Point Of Failure when one or more of the hardware or software components fails. | Proper high availability clustering should be setup for each tier.  Setup load balancer to improve availability after clustering. |
| Sensitive information | Information are being stored in client PCs without proper encryption.  Information are being transmitted over FTP in the clear from Mainframe to SHS. | Use Asymmetric Keys (public key) to encrypt data stored in client side.  Use SFTP instead of FTP. |
| Application Server | The location of application server is in DMZ, more ports on the inner firewall needing to be opened which largely undermines the value of the DMZ. | Place the application server in internal zone. |
|  |  |  |

**Use this page if your answers cannot fit in the above boxes.**