|  |  |
| --- | --- |
|  | CIS-1290 Principles of Information Security |

Topic 4 Part 3

|  |  |
| --- | --- |
| To: | Mike MacDonald |
| From: | Christopher Sigouin |
| Date: | February 25, 2015 |
| Subject: | Risk Management Class Activity ( Part 3 ) |
|  |  |

This assignment assesses the “Risk Control” phase of the Risk Management process utilizing a pharmacy company profile. The prior stages of “Risk Identification” and “Risk Assessment” have been completed in order to produce the following data below.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Safeguard Determination Table** | | | | | |
| TVA Name | Control Strategy | Recommended Safeguard Description | Residual Likelihood of Occurence | Residual Impact Severity | Residual Risk Level |
| Human error or failure / Data entry errors / Pharmacist | Defend | Increased system confirmation of data entries and annual training sessions |  |  |  |
| Human error or failure / Data entry errors / Student Temp Employee | Defend | Strong mentorship program |  |  |  |
| Human error or failure / Data entry errors/ Prescription delivery personnel | Accept | Data entry errors for the nature of the asset are acceptable |  |  |  |
| Quality of Service deviations from service providers / No access to assets / Process of interaction with HIAL ( Pharmacy Network ) | Mitigate | Implementation of IRP and DRP to maintain consistent availability. Use of backup services for example. |  |  |  |
| (1.a) Software attacks / Malware infections / Process of interaction with HIAL ( Pharmacy Network ) | Defend | All data scanned prior to entry into the local system. |  |  |  |
| (1.b) Software attacks / Malware infections / Process of interaction with HIAL ( Pharmacy Network ) | Mitigate | Processes implemented through IRP and DRP in the case of infection |  |  |  |
| Missing, inadequate or imcomplete organizational policy or planning / Improper exchange of information / Process with PoS: Initiating client transaction and client usage | Transfer | Ensure proper safeguards in place with PoS system in the event that information is provided to an unauthorized individual |  |  |  |
| Human error or failure / Data handling issues / Local Database: Patient Information, prescriptions, inventory, orders, professional info bulletins | Defend |  |  |  |  |
| Missing, inadequate or incomplete organizational policy or planning / Backup procedures / Local Database: PoS ( includes inventory, accounting , sales trends, pricing ) | Defend |  |  |  |  |
| Information extortion / Configuration issues / TELUS Assyst Rx software ( local system ) | Transfer |  |  |  |  |
| Missing, inadequate or incomplete controls / Unsecured access / TELUS Assyst PoS system software | Defend |  |  |  |  |
| Software attacks / Email systems / Miscellaneous applications ( Office suites, email systems, etc ) | Defend |  |  |  |  |
| Technical hardware failures or errors / Firmware failures / Servers ( Both TELUS Assyst Rx software and TELUS Assyst PoS system ) | Transfer |  |  |  |  |
| Forces of Nature / Destruction of hardware / Networking Equipment / | Mitigate |  |  |  |  |
| Theft / Risk of being stolen / Removable Media ( Backups, documentation, etc ) | Terminate |  |  |  |  |