Assignment # 2 Discussion Points

1. Risk Statement -> “so what” question, what can eventually go wrong and the consequences? e.g. weak password control; pervasiveness of privileged account assignment; lack of system patching policies and procedures, etc.,

Example One: “*Loss of critical company information due to unethical matters related to ADP payroll reporting efficiency could result in reputational damage to the company or potential litigation against the company*.”

Example Two: Not a risk statement, it’s a description of controls - “*Policies that govern crucial aspects of OS activities should be reevaluated on current basis, making sure that the procedures and particular activities are achieving their objectives. Policies and Procedures that do not account for changing environment create loopholes that can be abused by external entities..”*

1. Rating Rationale – Explaining risk rating from “Likelihood” and “Impact” aspects
2. Inherent Risk Rating – Impact/Likelihood/Overall; DO NOT take control into consideration.

Good Example: “*Inherent risk is medium because it is very difficult to account for every single scenario when writing policies and procedures (and it would not be reasonable to do so). Policies and Procedures should balance the level of control with the level of productivity, leaving some degree of flexibility to the employees.*”

Example: “*The server is accessed by an unauthorized user which could lead to data corruption or theft.*” - Not risk rationale

Example: “*Lack of scheduled updates and maintenances creates security vulnerabilities.*”

1. Why is “High” risk
2. Assessing the “Controls”
3. Expected Control vs. Current/Actual Control
4. Information gathering
5. Separate different type of controls; One risk can be mitigated by multiple controls; Primary vs. secondary controls (partial controls)
6. Control Statement

Example: “*Currently the policies and procedures are reevaluated by the IT department every 3 months.”*

Example: “*AC5 Output Review, Reconciliation and Error Handling AC4 Processing Integrity and Validity*.”

1. Assess the “Design of the controls” – Adequate or inadequate
2. Testing the “Operating Effectiveness” of the control – Effective or Ineffective or Inconclusive
3. Why it’s important to assess the “Inherent Risk” accurately?