Deanne Mitchill B. Agir BSIT - IV

Instruction: Answer the following questions comprehensively. Your answers will be graded based on coherence and overall presentation of ideas. The maximum points for each question is 50 points.

1. At which phase/phases in the SDLC should the IT auditor participate? What level of participation does he/she need to perform?

- The IT auditor should be included in the SDLC development process so that they can present the risks that will arise from developing their SDLC. The level of their performance participation must be at its highest level for the group creating their SDLC to acknowledge the IT auditor's work.

2. As an IT auditor doing risk assessment, will you recommend to the IT manager/management that once an employee's services had already been terminated from the organization, his/her access privileges should also be removed from the system? Why or why not?

- Due to the possibility that they could leak sensitive company information and to make it simpler to maintain the staff who still has access to the services for their employees, I think their access credentials should be revoked. Another factor would be the question of why the individual would continue to work for the company if their contract had already expired.

3. In IT auditing, how important is it for findings to be communicated to the management? Cite at least 2 examples.

- Because of the information's value and potential to influence how management develops, an IT auditor's conclusions are very significant. For instance, if the IT auditor identifies a potential technology risk, this could have a negative impact on how management develops. Another illustration may be the management of the complete IT information processing structure; it's possible that this structure needs to be rebuilt in order to process information more effectively.

4. What are the key success factors for effective project management? Give an example per factor.

A. Develop clearly defined plans with assigned responsibilities and accountabilities.
   - Each group member is responsible for a different aspect of the project and does everything in their power to see it through to completion.
B. Agree on the project goals.
   - The group should decide on what would they like to develop and achieve the goals they want
C. Manage the project scope effectively.
   - When developing the project, the group must make sure that they won't forget their scope and that the group can see their scope in their developed project.
D. Make sure you have management support.

- When a team member suffers with a task, management steps in to provide assistance so that the other team members can work with the struggling team member to complete the assignment as quickly as feasible.

E. Cultivate constant effective communications.
   - When making the capstone project, the group must ensure proper communication in order to avoid missing any updates coming from another member.

5. The two important elements in any software development are time and cost. When employing adaptive SDLC, how many times do you think revisions of the software product will be made?

- How well the SDLC goes will affect the revisions since you can't assume that "cost" means money or any other financial related matter, it could be the cost of revisions is "time," a "person" not able to do the assigned their assigned task, or many other things that can be considered as a "cost." Having the "time" to ensure that there will be fewer revisions in the SDLC will be another factor

6. What is/are the risks to the organization of not having a comprehensive business continuity plan in place in the event of an emergency?

- The risks of an organization not having a thorough business continuity plan, particularly in the event of an emergency, include not knowing who will be in charge in the event of an emergency, what their backup plan will be if a risk causes the organization a lot of damage, and who will be liable for any damages if a risk has already occurred and not been resolved.

7. Provide at least two examples of information security controls within the following management processes:

a. Vulnerability
   -
b. Threat
c. Trust
d. Identity
e. Incident