**Quiz**

**Name:………………………. ID:……………………. Section#:….**

|  |  |  |  |
| --- | --- | --- | --- |
| **#** | **A** | **The answer** | **B** |
| 1 | It involves splitting tasks among employees to reduce the chance of fraud. | **2 & 4** | Role-Based Access Control (RBAC) |
| 2 | It can help facilitate SoD by ensuring that a single user cannot approve their own changes assuming they are of a critical nature. | **1** | Separation of Duties |
| 3 | The principle that creates a balance between security and usability by minimizing the attack surface and enhancing operational performance. | **5** | Collusion |
| 4 | It assigns permissions based on users' roles within the organization. | **3 & 6** | Principle of Least Privilege |
| 5 | SoD enforces that two or more individuals would have to team up to perpetrate cyber mischief in the organization. |  |  |
| 6 | Focuses on providing employees with the account privileges they need. |  |  |
|  |  |  |  |

**Q1: Match the correct answer from column A to column B: 3 points**

**Q2: Put (T) for correct sentences and (F) for wrong sentences: 2 points**

1. Having Just-in-Time privileges and hardcoded credentials helps to implement the principle of Least Privilege. ( **F** )
2. An example of a role setup that enforces SoD is having an admin role that can approve requests to perform critical processes, execute them as well as audit them. ( **F** )
3. A SoD violation/conflict is when a person has the required roles to perform a combination of important activities in a process sequence. ( **T** )
4. An example of a role setup that enforces SoD is having separate roles for purchasing and approving the purchase, where a single user cannot do both. ( **T** )
5. Benefits of implementing the principle of least privilege include having limited malware propagation and better system stability. ( **T** )
6. A proper SoD can be accomplished by having the individual responsible for information security report to the chairman of the audit committee or by using a third party to monitor security and conduct surprise audits and testing. ( **T** )