Topic 6 Discussion 1

A recent procedure was put into place by the director of IT. However, you notice an inherent flaw in the procedure that could cause untold damages to the systems in place costing the organization an excessive monetary loss. How would you approach the director to ensure they are aware of the issue? What policy or procedures would you recommend implementing to ensure a validation process is in place and flaws in the procedure or policy are identified before implementation?

Hello Class,

Approaching the director of IT about a significant flaw in a newly implemented procedure requires a tactful and constructive strategy. First, I would schedule a private meeting to discuss my concerns, ensuring that the conversation is framed positively and focused on the organization's best interests. During the meeting, I would clearly articulate the specific flaw I’ve identified, providing concrete examples of how it could lead to potential damages and excessive monetary loss. It’s essential to present this information factually and without assigning blame, emphasizing the importance of safeguarding the organization’s assets and reputation.

To prevent similar issues in the future, I would recommend implementing a validation process that includes several key policies and procedures. Firstly, establishing a formal review process for all new procedures before implementation is crucial. This could involve a cross-functional team that includes representatives from IT, security, compliance, and relevant business units to evaluate the potential impacts and risks associated with the proposed changes(PowerDMS, 2020). Secondly, conducting pilot testing of new procedures in a controlled environment can help identify flaws before full-scale deployment. Additionally, instituting regular audits and feedback loops post-implementation can ensure that any unforeseen issues are quickly addressed(Unic, 2023).

References:

Kail, E., Nagy, A. R., Fleiner, R., Bánáti, A., & Ernő Rigó. (2025). Low-impact, near real-time risk assessment for legacy IT infrastructures. *International Journal of Information Security*, *24*(1). https://doi.org/10.1007/s10207-024-00971-4

PowerDMS. (2020, December 22). *Why it is important to review policies and procedures*. Www.powerdms.com. https://www.powerdms.com/policy-learning-center/why-it-is-important-to-review-policies-and-procedures

Unic, V. (2023, May 15). *Vulnerability Testing: Methods, Tools, and 10 Best Practices - Bright Security*. Bright Security. https://www.brightsec.com/blog/vulnerability-testing-methods-tools-and-10-best-practices/