Adrien Protzel

Thought questions

1. What audit objective is addressed by this interview?
    a. Audit objective from FISCAM CM.03.02:
        i. Determine whether critical updates and patches for the PaaS ERP system's cloud-deployed components, including those within containers, are implemented timely and whether unsupported information system components within these containers are promptly replaced to ensure system security and operational integrity, as managed by BigU using the provider's templates and update scripts.

    b. General control objective:
        i. Determine whether BigU's IT systems and processes are effectively updated and managed to ensure overall security, integrity, and compliance with current standards and regulations.

2. Identify two or three negative events or conditions that might arise if controls are not effective here?
    a. Security Breaches: If critical updates and patches are not implemented in a timely manner, the system may become vulnerable to cyber-attacks. These vulnerabilities can be exploited by malicious actors to gain unauthorized access to sensitive data, such as customer information, financial records, and intellectual property. This can lead to significant financial losses, legal penalties, and severe damage to the organization's reputation.

    b. Data Loss or Corruption: If data within the containers is not regularly backed up, there is a risk of losing new data during updates or system failures. Additionally, the presence of fake or corrupted data can compromise the integrity of the database, leading to inaccurate business decisions and operational disruptions. Ensuring regular backups and data integrity checks is crucial to prevent these issues and maintain reliable system performance.

3. Identify one of more controls/management processes you think should be in place to address those risks.
    a. Backup and Recovery (CP.02.01): To protect against data loss and corruption, regularly back up data and implement an effective recovery process. This can also roll back some attacks that take down the system or inject bad data.

4. Identify three questions the auditor might want to ask next. Remember: auditors should ask relevant (or at least potentially relevant) questions.
    a. Verification of Updates: “Can you provide documentation or logs that detail the recent updates and patches applied to the ERP system’s cloud-deployed components?”
    b. Backup Testing: “Have these containers been tested by rolling back the system to a previous container?” “How long are these containers retained, and are they ever disposed of or recycled?”
    c. Configuration Management: “What systems or tools do you use to ensure your containers are compliant with security policies and that they are integrated into your system seamlessly? Can you provide specific examples?”