Adrien Protzel

BigU Case 1

Draft 1

Identify and explain an area of IT risk

Elevated Access to Shared Resources:

This area of IT risk involves controlling elevated permissions for users, accounts, processes, and systems across an IT environment. This aligns with the principle of least privilege, aiming to limit access to only what is necessary for each entity. The control objective, “Accounts with administrative or elevated access to shared resources (privileged accounts) are controlled and monitored to ensure they are used only for authorized activities,” highlights the importance of managing these powerful accounts. The concern is that higher privileged accounts have extensive access to the system, and as noted, “Compromise of accounts with administrative control over IGA, cloud service, or network components could be devastatingly impactful as nearly all other security controls could be disabled.” This underscores the critical need for stringent controls over privileged access to protect the integrity and security of BigU’s IT environment. The principle of least privilege helps by limiting any entity or account to the bare minimum functionality it needs to complete its tasks. This means that general user accounts would not have administrative access, and certain admin accounts would be limited to specific functions to prevent excessive access to sensitive data or critical functionalities.

Identify and explain relevant controls

Privileged Access Management (PAM):

This control ensures that only authorized users and accounts have access to critical system data and functionality, preventing unauthorized access that could lead to internal attacks or fraud. This involves defining required responsibilities and privileges for each role to ensure that each user, account, and function only has access to what it should. BigU implements this control by identifying roles that require elevated access, adjusting their directory settings, and reviewing and approving requests from those accounts. They also ensure secure user access by implementing multi-factor authentication and continuously recording and monitoring usage. “Roles that require such access are identified, requests for access are reviewed and approved, user directory settings are adjusted, appropriate policies for passwords and multi-factor authentication are created and enforced, usage is recorded and monitored.”

Identity and Access Management (IAM):

This focuses on user authentication and credentials, ensuring secure access to systems, data, and user accounts. BigU simplifies the authentication process as described here, “BigU’s IAM processes facilitate Single Sign On (SSO) using three tools: Microsoft’s Active Directory, an identity governance and administration (IGA) system, and dual authentication services.” These credentials are kept up to date by implementing tools for password management, enforcing regular password changes, and using multi-factor authentication.

Cloud Service Management:

Cloud services ensure that cloud services are securely configured and managed to protect data and systems from external threats. BigU strengthens their enterprise resource planning (ERP) by using a Platform as a Service (PaaS) to externally manage their cloud data. This approach ensures that their cloud environment is kept up to date and compliant with current standards. Both the cloud provider and BigU need to interact and secure their ends of the cloud system by reviewing and adhering to the cloud provider's shared responsibility model, ensuring both parties fulfill their security obligations. "You're responsible for securely configuring and managing your compute (virtual hosts, containers), storage (object, file, local storage, block volumes), and platform (database configuration) services."

Disaster Recovery and Business Continuity:

Disaster Recovery and Business Continuity ensure that in addition to cloud service management, the PaaS also helps with recovery in the event of a disaster, maintaining operational continuity in the system. "BigU benefits from several key services including database as a service (DBaaS), Container Services, and Disaster Recovery as a Service (DRaaS)." This ensures that data is regularly backed up and can be restored in case of data loss. The process involves scheduling regular backups, using secure storage solutions, and regularly testing the backup data to ensure it is not corrupted, missing, and that the system accepts it. "Frequent and remotely distributed backups of the database logs allow BigU to claim that no more than 15 minutes of data would be lost in a disaster." This directly supports BigU's recovery point objectives (RPO) and recovery time objectives (RTO) to minimize data loss and downtime.

Identify and explain how an auditor might assess

To assess the IT audit case for BigU, an auditor would need to understand the scope and objectives of the audit. They would identify areas of potential risk and the main concerns of the university. The auditor would review control objectives and existing controls to determine their effectiveness. Specifically, they would examine processes for managing privileged accounts, ensuring multi-factor authentication is enforced, and monitoring logs of privileged account activities. The auditor would also assess the cloud provider's security responsibilities and confirm BigU's processes for updating ERP containers, ensuring both are compliant with standard regulations. Additionally, they would evaluate identity and access management (IAM) processes, check the integration of Single Sign-On (SSO) tools, and verify disaster recovery capabilities and plans. Throughout the audit, the auditor would use inspection, testing, confirmation, and inquiry to gather evidence and provide assurance that controls are effective and risks are mitigated.