BigU Case 1

Draft 2

# Identify and explain an area of IT risk

### Elevated Access to Shared Resources:

This area of IT risk involves the potential for unauthorized use of elevated permissions granted to users, accounts, processes, and systems across an IT environment. The risk is that these elevated permissions could be exploited, leading to unauthorized access and potentially severe consequences for the organization.

For example, if an account with administrative control over identity governance and administration (IGA), cloud services, or network components is compromised, it could disable nearly all other security controls, resulting in significant data breaches or system failures. 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 principle of least privilege helps mitigate this risk by limiting access to only what is necessary for each entity, thereby reducing the potential impact of a compromised account.

# 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. 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 (MFA) and continuously recording and monitoring usage. For example, roles that require such access are identified, requests for access are reviewed and approved, user directory settings are adjusted, appropriate policies for passwords and MFA are created and enforced, and 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 by facilitating 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 MFA.

### Cloud Service Management:

This control ensures 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.

### Disaster Recovery and Business Continuity:

This control ensures 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.

For example, an auditor might perform the following procedure:

* Inspection: Review the configuration settings of privileged accounts to ensure they adhere to the principle of least privilege.
* Testing: Test the effectiveness of multi-factor authentication by attempting to access systems with and without MFA.
* Confirmation: Confirm that all privileged access requests are reviewed and approved by appropriate personnel.
* Inquiry: Interview IT staff to understand the procedures for monitoring and responding to suspicious 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.