Adrien Protzel

BigU Case 2

Draft 1

Identify and explain an area of IT risk

Disaster Recovery and Data Backup:

This area of IT risk involves ensuring that an organization can recover its IT systems and data in the event of a disaster, such as a natural disaster, cyberattack, or system failure. Effective disaster recovery aligns with the principle of business continuity, aiming to minimize downtime and data loss. The control objective, “Critical systems and data are backed up regularly and can be restored promptly in the event of a disaster,” highlights the importance of having robust disaster recovery plans and backup procedures. The concern is that without proper disaster recovery measures, an organization could face significant operational disruptions and data loss. As noted, “Failure to restore critical systems and data promptly could lead to severe operational, financial, and reputational damage.” This underscores the critical need for stringent controls over disaster recovery processes to protect the integrity and availability of BigU’s IT environment.

Identify and explain relevant controls

Defined RPO and RTO:

In the BigU case, the defined Recovery Point Objective (RPO) and Recovery Time Objective (RTO) are critical components of the disaster recovery strategy. The RPO is set at 15 minutes to ensure that no more than 15 minutes of data is lost in the event of a disaster: “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.” The RTO, set at two hours, ensures that the system is restored within two hours of a disaster: “The system can be back up in two hours – recovery time objective (RTO) – even if services need to be transferred to the backup datacenter.” This integration of frequent backups and robust recovery procedures ensures minimal data loss and swift system restoration, maintaining the integrity and availability of BigU’s IT environment.

DRaaS with cloud hyper-scale facilities:

Disaster Recovery as a Service (DRaaS) combined with the cloud provider’s hyper-scale facilities is a crucial component of BigU’s disaster recovery strategy. “BigU benefits from several key services including database as a service (DBaaS), Container Services, and Disaster Recovery as a Service (DRaaS).” This setup provides BigU with robust storage and recovery processes to mitigate data loss from any source. The cloud provider’s hyper-scale facilities, which are extensive data centers managed by the provider, offer well-tested disaster recovery capabilities without requiring BigU to invest in or manage the infrastructure. This combination ensures that BigU can rely on advanced, scalable infrastructure and services to maintain the integrity and availability of its IT environment in the event of a disaster.

Backup and storage of system container configurations:

In addition to all of the DRaaS infrastructure, an extra control is implemented to strengthen disaster recovery and business continuity. While the DRaaS with cloud hyper-scale facilities primarily serves as a place to hold the data, this control ensures that the data is being saved and stored in these cloud systems. This control involves regularly backing up the configuration details of the system containers, which are essential for the operation of BigU's IT environment: "The configuration details of the system containers are backed up and stored where they can be initialized in an alternate data center in the unlikely event that the primary datacenter shuts down." Regular backups ensure that the most current configurations are always available for recovery, capturing any changes or updates made to the system configurations so that any recovery will use the most up-to-date version before the data loss or disruption. These backups are also stored in remote locations, separate from the primary datacenter, providing geographic separation that protects the backups from being affected by the same natural disaster. In the event that the primary datacenter shuts down, the backed-up configuration details can be quickly initialized in an alternate datacenter, allowing BigU to restore its IT environment and resume operations with minimal downtime.

Identify and explain how an auditor might assess

To assess the IT audit case for BigU, an auditor focusing on disaster recovery controls and plans 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 related to disaster recovery. The auditor would review control objectives and existing controls to determine their effectiveness in ensuring business continuity. Specifically, they would examine the processes for backing up and storing system container configurations, ensuring that these backups are regularly updated and stored in remote locations. The auditor would also assess the effectiveness of the Disaster Recovery as a Service (DRaaS) and the cloud provider's hyper-scale facilities, verifying that these services provide robust and well-tested disaster recovery capabilities. Additionally, they would evaluate the defined Recovery Point Objective (RPO) and Recovery Time Objective (RTO) to ensure that they meet the university's requirements for data loss and system restoration times. Throughout the audit, the auditor would use inspection, testing, confirmation, and inquiry to gather evidence and provide assurance that disaster recovery controls are effective and risks are mitigated.