­

**DGN2 TASK 1: Cloud Security Implementation Plan**

Barbara Garcia

011883626

College of Information Technology, Western Governors University

May 3, 2024

**A. Executive Summary**

After analyzing the business requirements and comparing it to the current security environment, it was determined that improvements to security need to be made. The company’s business requirements are as follows: Maintain compliance with regulations and standards to support the success of federal contracts; maintain ability to provision, configure and operate cloud virtual servers as needed; implement a cloud instance that can support encryption of data at rest and in transit; Accounting, Marketing and IT departments should each have their own Azure Resource Group containing only resources associated with their respective department; each migrating department should have its own Azure Key Vault for least privilege; Azure Key Vualt access policies should be configured for departmental users only; IT department is responsible for performing and verifying backups; cloud servers should have a RPO of 1 day and RTO of 36 hours with backups conducted at 7pm EST daily; Instant recovery snapshots should be maintained for 3 days and daily backup points for 45 days;all virtual machines should be backed up using a Single Recovery Vault under a new backup policy named SWBTL; and tags can be used to identify resources belonging to each department.

Many settins in Azure are misconfigured and do not align with business requirements nor do they comply with regulatory requirements. Configuration changes are necessary.

**B. Proposed Course Of Action**

Given the business requirements of the company, the appropriate service model is Infrastructure as a Service via Hybrid Cloud.

Applicable regulatory compliance directives that apply to the company are FISMA and PCI DSS.

Security benefits of transitioning to this service model include increased security, reduced downtown, the ability to dynamically scale, ease of innovation and boosted speed. (*What Is IAAS - Advantages and Disadvantages | Cloud Computing | CompTIA*, n.d.)

Challenges of transitioning to this service model include complex integration, process changes, limited customization, vendor lock-in and runaway inventory.

**C. Role Based Access Control**

**C1. RBAC Recommendations**

Implementing role-based access controls for marketing, account, and IT resource groups will increase security and facilitate future configuration changes.

One recommendation for role-based access controls in the Azure environment is that each resource group should only contain resources associated with its respective department.

A second recommendation for role-based access controls is that each migrating department should have its own resource group in Azure.

A third recommendation is that, since IT is responsible for performing and verifying backups, those items should be assigned to their role.

**C2. RBAC Configuration**

1. Moved marketing VM to marketing Resource GroupA screenshot of a computer

Description automatically generated

2. There is no NetworkWatcherRG Department. Deleted Resource Group

A screenshot of a computer

Description automatically generated

3. Added role assignment to IT resource group

A screenshot of a computer

Description automatically generated

**D. Encryption**

**D1. Encryption Implementation**

One best practice per the business practice requirements is that each migrating department have its own Azure Key Vault. Accounting and Marketing were assigned to the wrong key vault. The settings changes below reflect assigning the correct departments to their corresponding key vaults.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Another best practice for encryption in the Azure environment is that only users from each department should be able to access that department’s corresponding key vault.

A screenshot of a computer

Description automatically generated

**D2. Encryption Recommendations**

One recommendation for how key vaults can be used for encryption is to enable ‘Encryption at Host.’ This setting causes data to be encrypted at rest and when it goes to the storage device, it is encrypted in transit.

Another recommendation for encryption in the Azure environment is to enable “Azure Disk Encryption.” This encrypts all data stored in the Azure environment when it is at rest.

**E. Back Ups**

**E1. File Backup Configuration**

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

**E2. File Backup Explanation**

Establishing a new single recovery vault for virtual machines and applying a backup policy named SWBTL meets the stated business requirements for backing up data.

Setting up standard backups to be conducted at 7:00pm Eastern Standard Time every day and maintaining instant recovery snapshots for 3 support business requirements by making a recovery point objective of one day and a recovery time objective of 36 hours possible.

**F. Division of Responsibility**

When operating on Azure with an Infrastructure as a Service model on a Hybrid cloud, there are shared responsibilities between the company and the cloud service provider. The company is responsible for most security controls over the operating system, implementing access controls, backing up data, and encrypting data. Azure is responsible for physical aspects of the cloud such as datacenters, hardware, storage network equipment, host servers and virtualizations.

**F1. Risks**

One risk assumed by the company under this model is data breeches. The impact of a data breech would be loss of reputation, financial consequences and potential regulatory fines.

Another risk assumed by the company under this cloud model is insider threats. The impact of insider threats is malicious access to internal resources, the potential for attacks to go unnoticed, data modification and data exfiltration.

A third risk assumed by the company is insufficient identity acess management and key management. The potential impact of this risk is account takeover and/or privilege escalation. This would allow an unauthorized person access to internal systems which could result in loss of confidentiality.

**F2. Compliance Recommendations**

Compliance is in important aspect of this company’s business requirements.

One recommendation to ensure compliance with the company’s cloud security posture is to use encryption. Encrypting data at rest and in motion will ensure confidentiality, which is important not only to the company’s business but also to remain compliant with regulatory requirements.

Another recommendation for compliance is to implement segregation of duties. This avoids any one person being able to conduct sensitive actions and increases security.

A third recommendation to ensure compliance is to enforce the use of a password policy. Implementing requirements that force users to comply with password length, complexity, history and age requirements makes identity access management more secure and lessens the likelihood of attacks like account takeover and privilege escalation.

**G. Potential Threats**

There are various potential threats that have the potential to impat the updated cloud solution of the company.

One of these potential threats is misconfiguration. In order to battle complacency and human failure, a mitigation for this threat is to use CIS benchmark to guide configuration.

Another potential threat is poor access control. In order to mitigate this threat, the company should use multi factor authentication with strong factors and require regular – reauthentication. *(CSI-MITIGATING-CLOUD-VULNERABILITIES)*

A third potential threat is exposure to shared tenancy vulnerabilities. This can be mitigated by enforcing strong encryption along with propertly configured, managed and monitored key management programs.

**References**

*What is IAAS - Advantages and disadvantages | Cloud computing | CompTIA*. (n.d.). CompTIA. https://comptia.org/content/articles/what-is-iaas

Timonera, K. (2023, December 19). *IaaS Security: Top 8 Issues & Prevention Best Practices*. eSecurity Planet. https://www.esecurityplanet.com/cloud/iaas-security/#:~:text=IaaS%20enables%20enterprises%20to%20expand,or%20adopting%20extra%20security%20services.

https://media.defense.gov/2020/Jan/22/2002237484/-1/-1/0/CSI-MITIGATING-CLOUD-VULNERABILITIES\_20200121.PDF

Roygara. (2023, November 2). *Enable end-to-end encryption using encryption at host - Azure portal - managed disks - Azure Virtual Machines*. Microsoft Learn. https://learn.microsoft.com/en-us/azure/virtual-machines/disks-enable-host-based-encryption-portal?tabs=azure-powershell