**Cloud Security**

Western Governors University

August 23, 2024

**A: Executive Summary**

Overview:

SWBTL LLC, a shipping company is rapidly expanding. Because of their level of demand and growth they are looking for solutions to scale in a secure manner. They consulted with a cybersecurity professional who introduced them to Azure, however when the consultant left the company employees were reporting several issues. Upon accessing the cloud, I noted several security issues, which I updated immediately to mitigate risk.

The company is weighing the pros and cons of continued migration to a cloud-based solution after this experience. In addition, they are determining what would be the best service model if they were to move forward with the cloud.

They are starting the process with three departments to determine whether migration would be feasible: IT, Accounting, Marketing.

The rising cost of computing power for a company that is now nationwide is making it very challenging to scale without the use of the cloud. It is also costing the company additional resources to secure the physical location and protect their business assets.

Azure is a great solution if used properly, as they have a lot of security tools and resources to help scale a growing business at a reasonable cost. It also transfers some of the responsibility and risk to the service provider, freeing up resources that would be used to secure a physical space. Logical segmentation of networks can also be accomplished relatively quickly.

Upon access to the cloud network I discovered the previous consultant had the majority of the resources in the IT group. They were not utilizing key vaults for encryption of data at rest or in transit. In addition, there was no policy in place to back up the company’s sensitive data.

Effective utilization of Azure cloud with the proper configurations will allow the company to increase their security posture and scale efficiently. We will also remain compliant with FISMA & PCI DSS while doing so (CMS Information and Security Privacy Group, 2023).

**B: Proposed Course of Action**

SWBTL has been growing at a rapid pace. Their services have already expanded nationwide with over 2000 employees. Because the company has grown so large, their attack surface has expanded. There are more ways for malicious attackers to gain access to their systems. In addition, they have more systems for attackers to gain access to. To accommodate the increasing demand, I am recommending a series of actions be implemented as soon as possible. This will minimize the amount of risk that SWBTL is exposed to. In addition, this will help the company to meet new and existing regulatory compliances.

I recommend that SWBTL use the IAAS (Infrastructure as a Service) model. This will allow the company to scale with increased demand and make the proper adjustments as necessary. In addition, there are regulatory compliances the company should adhere to. The company has expanded their business to contract with the Government, so it is important to comply with FISMA. In addition, they are handling customer credit card information, so they must comply with PCI DSS. The tools that will be presented through Azure will allow the company to configure their network accordingly. They will be able to create policies for backup. In addition, they will be able to use Azure specific tools for compliance management. By splitting their different departments into resource groups, they will be able to implement the principle of least privilege and provide access to only what is necessary. This will add a greater level of security to sensitive customer data.

**C1: RBAC Recommendations**

Currently it looks like the resources are in the incorrect resource groups. Many of the resources from other departments are inside of the IT department group. To implement the principle of least privilege it is important to give employees access only to the resources they need. Since there are three different departments it’s imperative that we separate these departments and provide access only to those that belong to the departments. To start we will separate all of the resources into three different departments: It, Marketing, and Accounting. After we have separated all the resources, we will assign users that belong to each department to their designated resources, so they will only be able to access what they need. We will also add key vaults into each department and assign RBAC policy, so we are able to add specific users as key contributors. This will help us to secure data by adding a level of encryption. Utilizing the Azure cloud will make identity access management more convenient for the company. I will also recommend as the departments begin to grow; employees are assigned specific roles within the department based on their job tasks.

**C2: RBAC Configurations**

Figure 1

IT Department – Resource Group

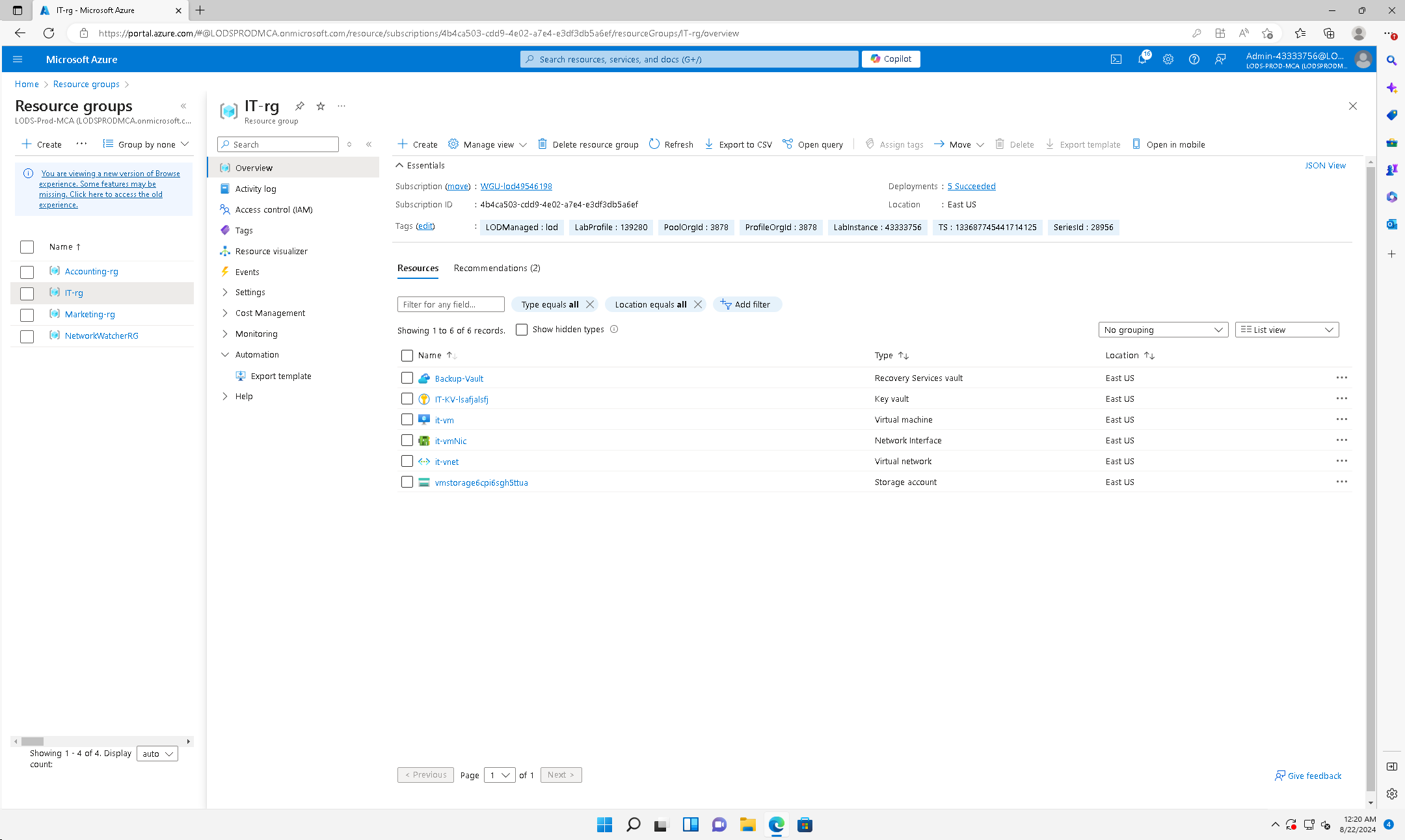


Figure 2

IT user – RBAC (IT Resources)

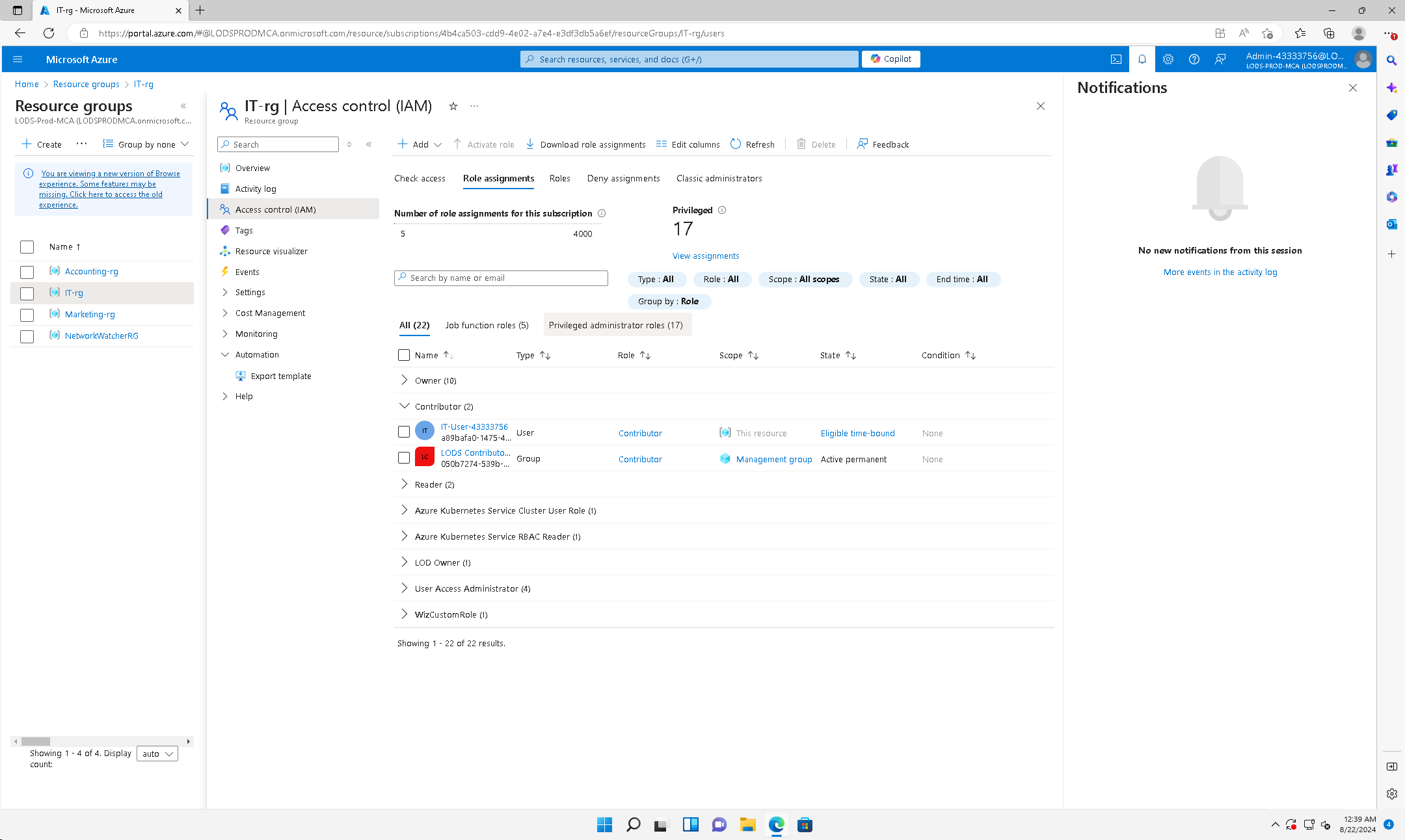


Figure 3

Accounting Department – Resource Group

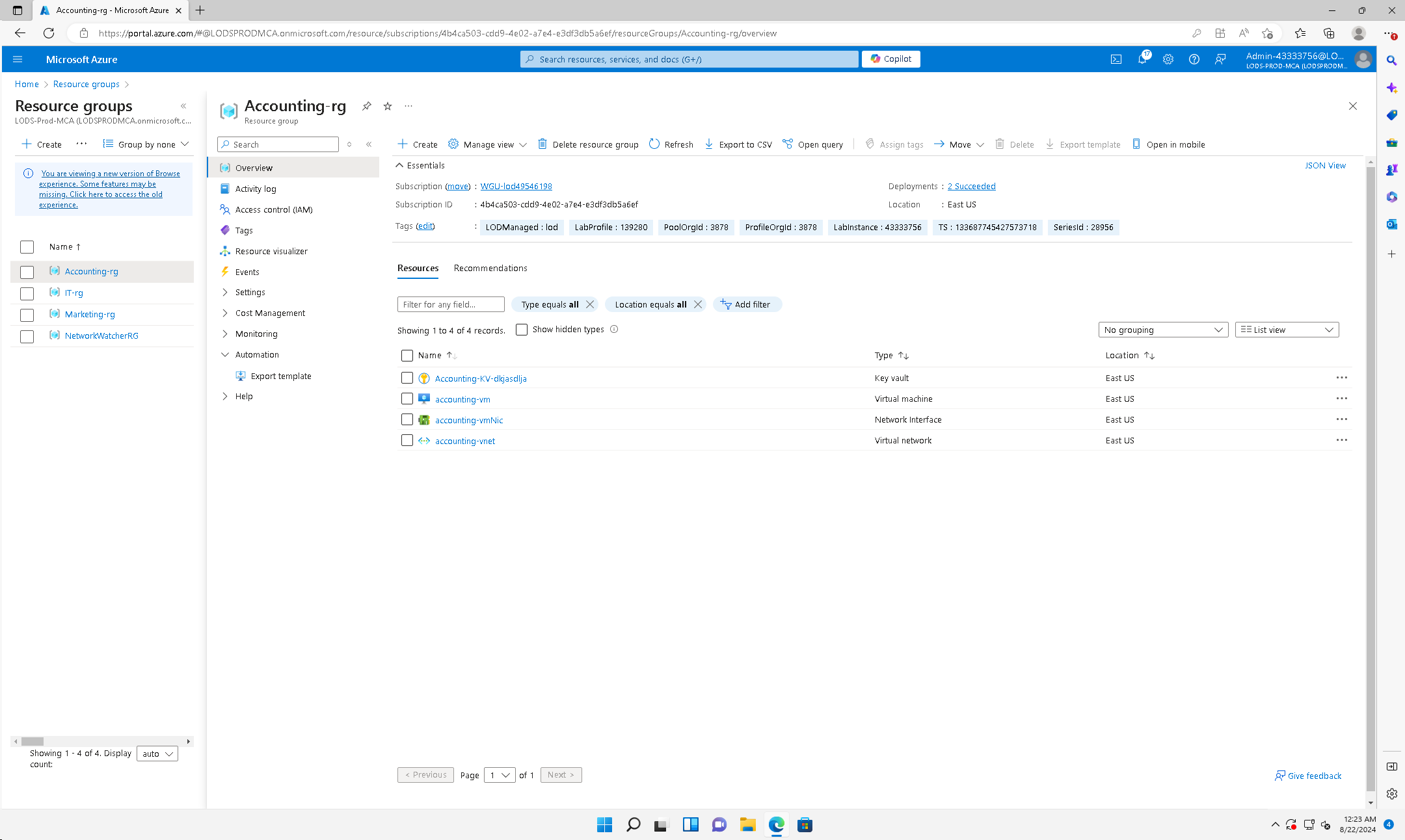


Figure 4

Accounting user – RBAC (Accounting Resources)

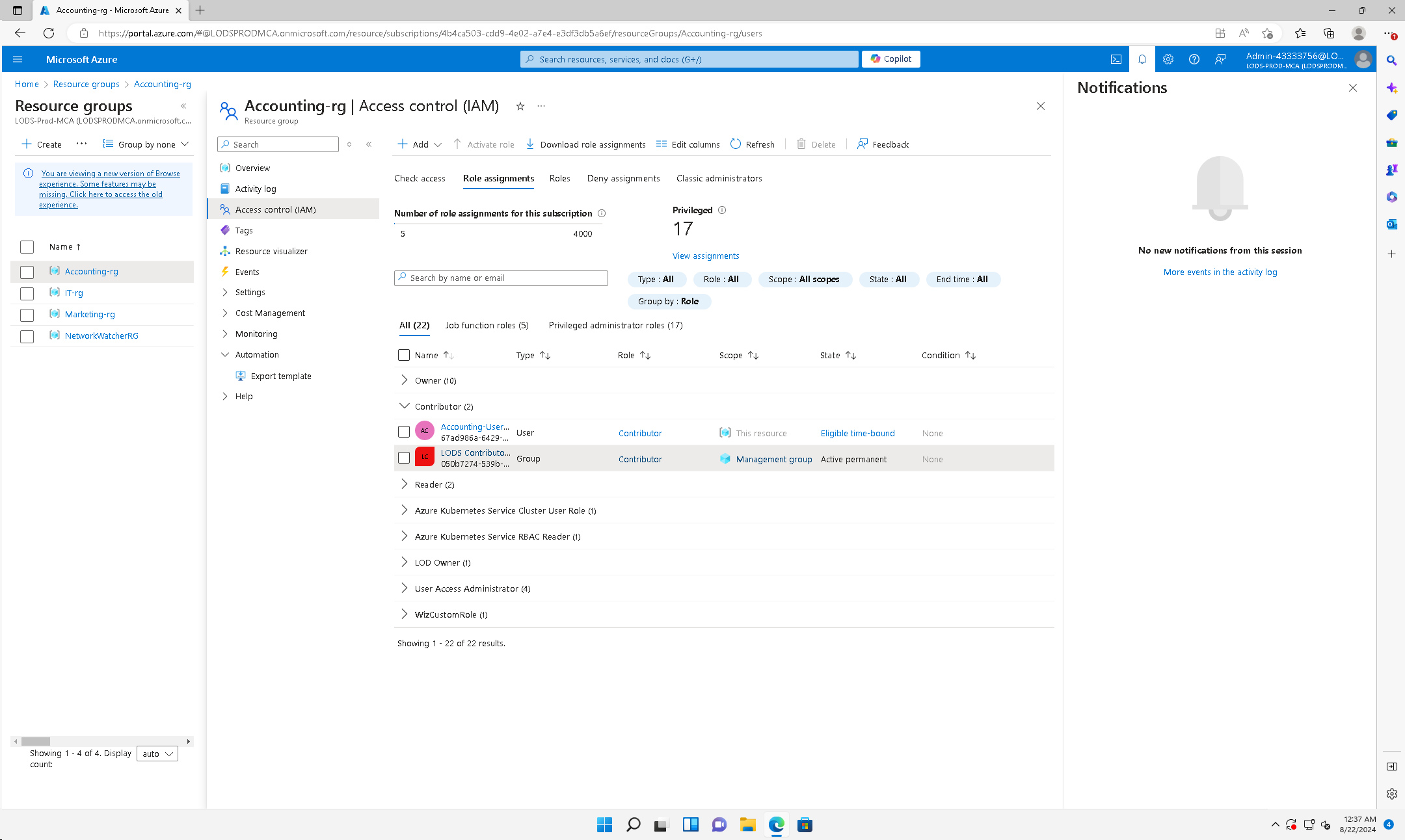


Figure 5

Marketing Department – Resource Group

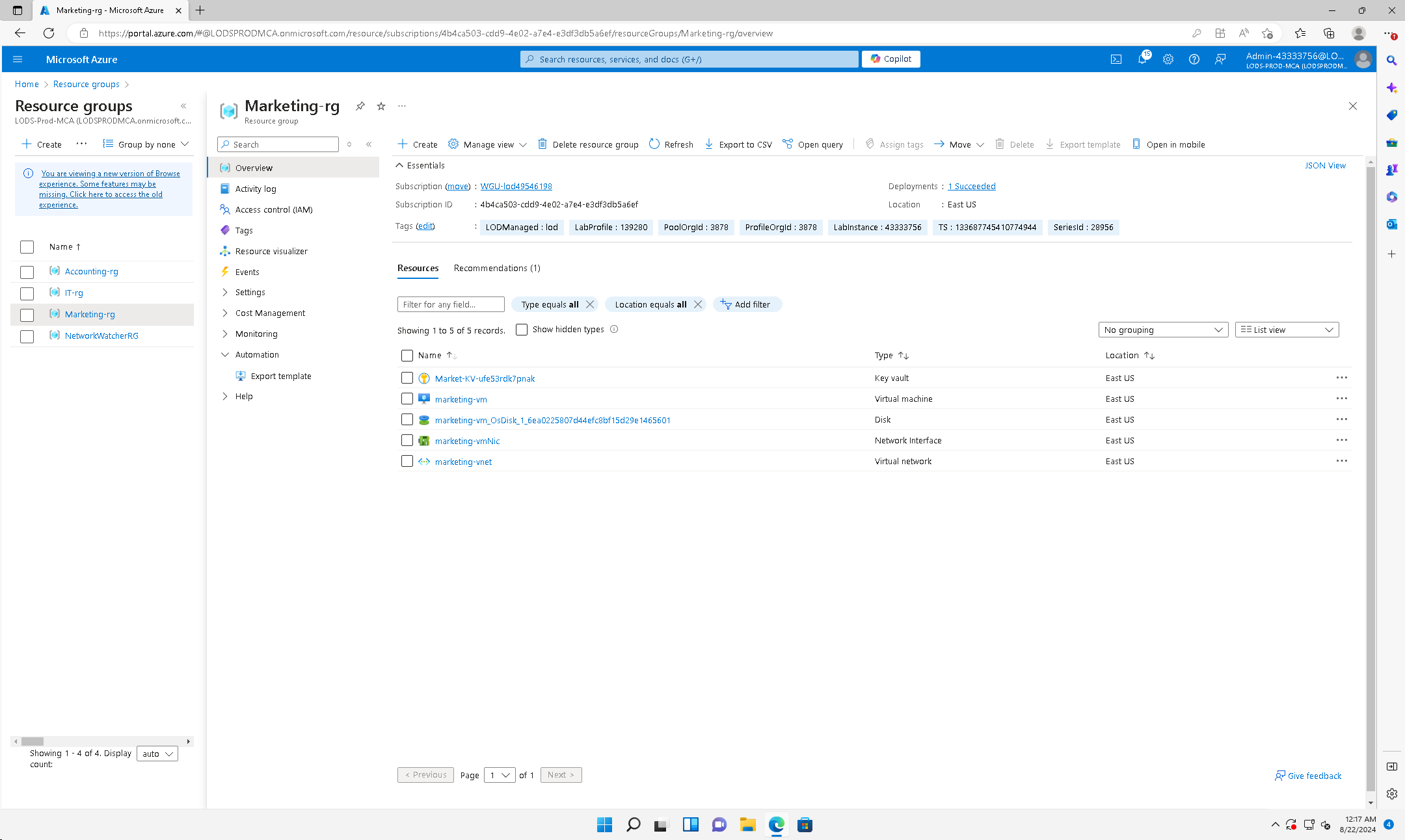
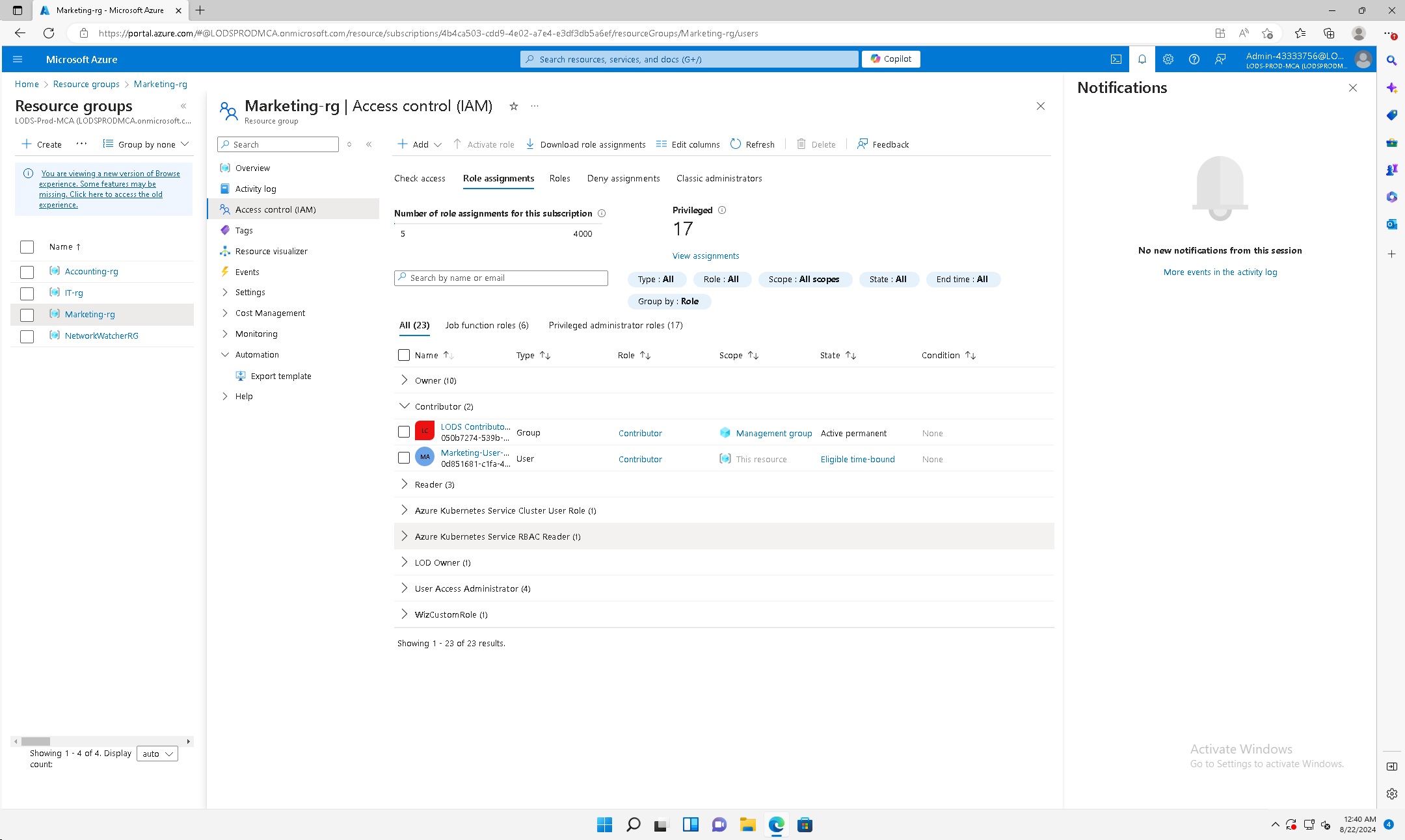


Figure 6

Marketing user – RBAC (Marketing Resources)



**D1: Encryption Implementation**

Figure 7

IT Department Key Vault – IT User (Key Vault Contributor)

A screenshot of a computer

Description automatically generated

Figure 8

Accounting Department Key Vault – Accounting User (Key Vault Contributor)

A screenshot of a computer

Description automatically generated

Figure 9

Marketing Department Key Vault – Marketing User (Key Vault Contributor)

A screenshot of a computer

Description automatically generated

**D2: Encryption Recommendations**

By placing an independent key vault in each department’s resources group we can add a greater level of security and comply with FISMA and PCI DSS. We recommend that the company use Azure storage to automatically encrypt data at rest, the key vault will store the keys which will decrypt the data (CMS Information and Security Privacy Group, 2024).

Since SWBTL has customer facing websites which process customer’s card information it is important that this data is encrypted. We can achieve this by utilizing SSL/TLS. We will store the certificates in Azure Key Vault and utilize these for encryption.

**E1: File Backup Configuration**

When I analyzed the cloud environment, SWBTL didn’t have a backup policy set in place. I’m highly recommending this feature, as it would allow the company to recover in a timely manner should a disaster occur. If any business interruptions or attacks occur, this will allow SWBTL to continue operations.

Figure 10

Backup Policy

A screenshot of a computer

Description automatically generated

**E2: File Backup Explanation**

By creating this policy, we can achieve our recovery point objective of one day. All servers will be backed up at 7 am eastern time every day to achieve our recovery time objective of 36 hours. In addition, recovery snap shots are maintained for 3 days, and backup points are maintained for 45 days. This will ensure that our business/regulatory requirements are met regarding recovery and backup.

**F: Division of Responsibilities**

With this model the company is transferring some responsibilities to Azure. When the company was smaller, they were responsible for all the physical devices and networking configurations. There would need to be safeguards to prevent physical access to servers and accessibility of data. With the IAAS model, Azure will be responsible for maintaining all the physical servers and ensuring physical security. They will also be responsible for the infrastructure and networking.

SWBTL will be responsible for properly configuring devices on the cloud. There is still a lot of room for error. The previous consultant placed all the machines in the same resource group and employees were complaining about being able to view everything. It’s important for companies to split their resources according to the principles of least privilege and to separate duties. For this model, an understanding of Identity Access Management is critical. It is important that users have the correct privileges. In addition, passwords and authentication should be configured properly. Azure is responsible for providing the framework and tools that allow for the configuration. If for any reason this framework has an error, it could impact the company utilizing the service.

**F1: Risks**

Risks associated with configuration could be from accidentally providing the wrong with employees or vendors with access to business-critical information. This could result in leaking proprietary information or even sensitive information about customers. Data loss regarding customer information which could result in a fine from PCI DSS. (UCSF Controllers office, 2023).

Azure is responsible for maintaining physical networks and deploying virtual networks appropriately. If the company misconfigures the network, this could allow malicious actors access and could even result in a DDOS attack which could interrupt business operations.

Another shared responsibility is encryption of data discussed earlier. Azure is responsible for maintaining tools such as Azure Key Vault, which helps to encrypt and decrypt data. If these tools fail, it would be less challenging for a malicious actor to view sensitive data, if they were able to intercept packets. Customers place orders with their credit card via websites.

**F2: Compliance Recommendations**

For SWBTL to maintain a strong security posture on the cloud they should take as many actions as possible to reduce the attack surface. This is one of the challenges that many companies face as they begin to grow rapidly. The adjustments that were made on the cloud will help them to get started.

Segmenting their networks by splitting their resources by department and assigning employees to groups based on their roles will strengthen the security posture. This is a logical representation of what happens with physical segmentation. I would also recommend Azure Firewall implementation and IP based access to further limit accessibility of sensitive data.

Introducing key vaults which store certificates that encrypt data via SSL/TLS, ensuring secure connections between devices. Encryption of data at rest in Azure Storage containers, which require keys stored in Key Vault. These also create a greater level of security posture.

Having a good backup policy to ensure you can recover in case a major disaster ever takes place is essential. It is important the software that Azure is using to backup is functioning properly. It is also crucial the policy is configured properly according to the business needs and data sensitivity.

**G: Potential Threats**

While the implementations in the cloud environment increase the security posture. There are still inherent threats. One of which is the level of access each user has. This could result in an insider threat. It is important to provide a list of all employees along with their roles and responsibilities. The list should be reviewed and updated regularly to accomplish the principle of least privilege.

The company also opens their business up to threats from malicious actors across the globe. Since they have moved business critical servers from three different departments onto the cloud, there is potential that someone can access these if they spot a weak configuration. Prior to this someone may have required physical access to a building to gain access to these servers. The company can mitigate risk with Azure firewalls and geographical based access policies.

The other threat the company faces is reliance on the CSP. If Microsoft Azure experiences issues this could affect the companies’ servers and impact business. A way to mitigate this is with Azure site recovery, and redundant servers if resources allow. There should be backup plans for continuity in case a disaster impacts operations.

There are many threats that can exist. It is important to stay up to date with trends and ensure all configurations are correct, and that servers and operating systems are up to date.

**H: Sources**

CMS Information and Security Privacy Group. (2024). Federal Information Security

Modernization Act. https://security.cms.gov/learn/federal-information-

security-modernization-act-fisma

UCSF Controllers Office. (2023). Understanding PCI DSS.   
 https://controller.ucsf.edu/how-to-guides/accounting-reporting/understanding-payment- card-industry-data-security-standard-pci