CLOUD SECURITY – D485

DGN1 TASK 1: Cloud Security Implementation Plan

Shane M. Deitle

Western Governors University

College of Information Technology, Western Governors University

November 7th, 2023

A: Provide an executive summary of the company's current security environment based on the business requirements given in the "Company Overview and Requirements" document.

SWBTL LLC, originating in 1977 as a local document and delivery service, has evolved into a nationwide operation with over 2,000 professionals. Facing constraints with leased data centers, cybersecurity concerns, and regulatory compliance, the company has decided to transition to the Microsoft Azure cloud environment. Key business requirements include the following:

1. Regulatory Compliance:
   - SWBTL LLC must maintain compliance with regulations such as the Federal Information Security Modernization Act (FISMA) and the Payment Card Industry Data Security Standard (PCI DSS) to support federal contracts.
2. Cloud Transition:
   - The company is migrating to Azure for its cloud needs, aiming to deploy and control multiple operating systems, virtual machines, and custom applications, with initial migrations including the marketing, accounting, and IT resource groups.
3. Data Security:
   - Encryption of data-at-rest and data-in-transit is crucial, following industry standards and regulatory requirements.
4. Departmental Isolation:
   - Each migrating department should have its own Azure Resource Group and Azure Key Vault to adhere to the principle of least privilege.
5. Backup and Recovery:
   - The IT department is responsible for backups, with a recovery point objective (RPO) of 1 day, daily standard backups, instant recovery snapshots for 3 days, and daily backup points maintained for 45 days.
6. Role-Based Access Controls (RBAC):
   - RBAC should align with the principle of least privilege for the marketing, accounting, and IT resource groups.

The departure of a disgruntled employee has raised security concerns, with reported data visibility across teams and unverified file and system backups. The Chief Information Officer aims to address these issues, minimize risk, and ensure compliance with regulatory requirements.

B: Describe a proposed course of action for a secure Azure cloud solution for the company, based on the given scenario, and include the following in your description: identification of the service model, applicable regulatory compliance directives, security benefits and challenges of transitioning to this service model.

To meet SWBTL LLC's security objectives in transitioning to Microsoft Azure, a recommended course of action involves opting for the Infrastructure as a Service (IaaS) service model. This model aligns with the company's requirements, allowing the deployment and control of multiple operating systems, virtual machines, and custom applications while maintaining flexibility and control.

The IaaS model will enable SWBTL LLC to have granular control over the virtualized infrastructure, supporting the diverse needs of the marketing, accounting, and IT resource groups. This model ensures compatibility with legacy authentication requirements, integration with the existing Active Directory structure, and support for internally developed software.

For regulatory compliance, adherence to the Federal Information Security Modernization Act (FISMA) and the Payment Card Industry Data Security Standard (PCI DSS) is paramount. Microsoft Azure, with its robust compliance framework, facilitates alignment with these standards, offering a secure environment for handling government contracts and card transactions.

The IaaS model provides enhanced security benefits such as customizable security configurations, controlled access to resources, and the ability to implement encryption measures. However, challenges include the need for diligent management of security configurations and updates to ensure ongoing compliance. Continuous monitoring and proactive security measures will be essential to mitigate potential risks associated with the dynamic cloud environment.

By adopting IaaS, SWBTL LLC can leverage the scalability and flexibility of Azure while maintaining a secure and compliant cloud environment. Ongoing monitoring and adherence to best practices will be crucial to ensuring the sustained security of the company's cloud infrastructure.

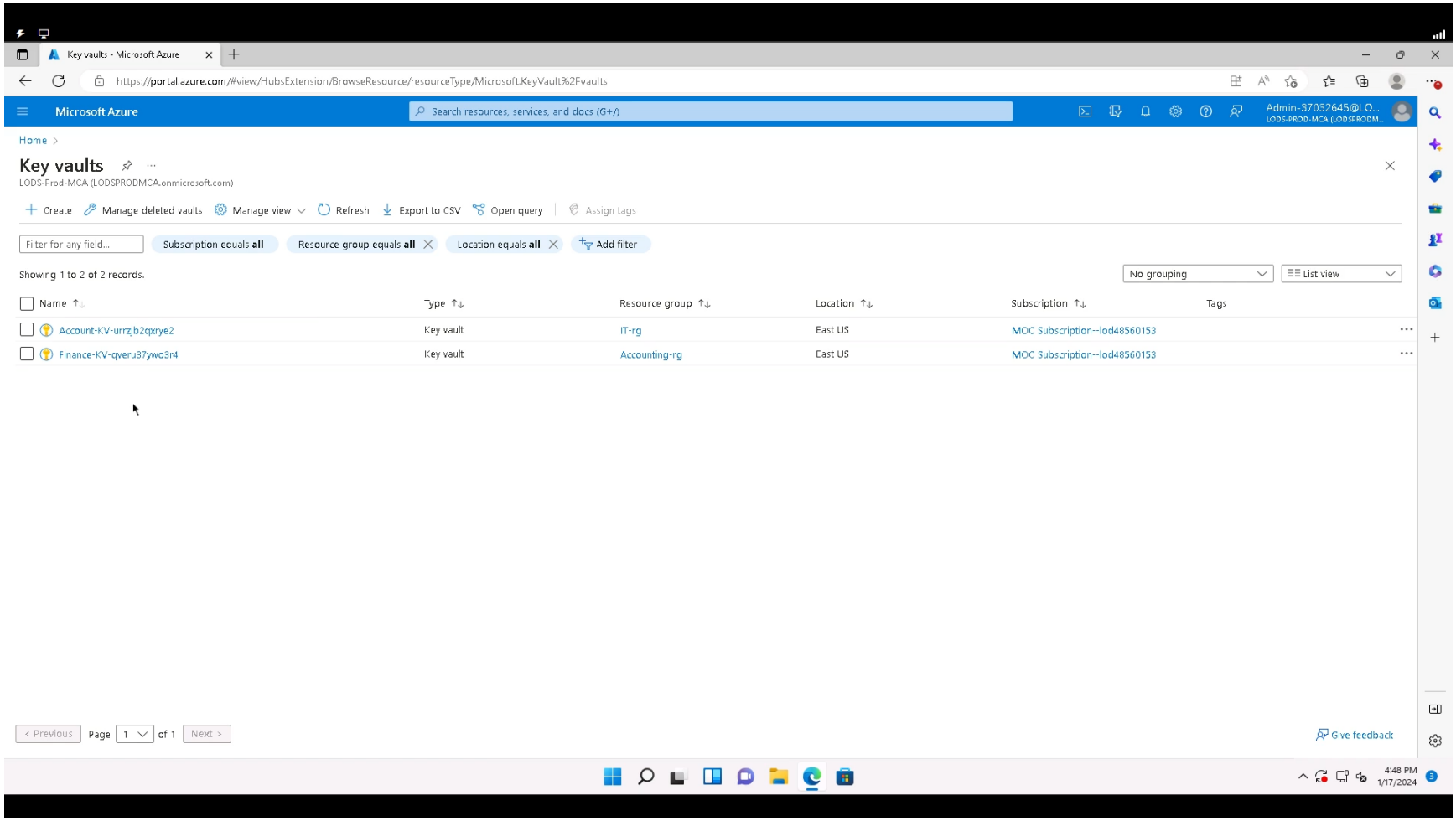
C: Analyze the current state of role-based access controls in the cloud lab environment for the marketing, accounting, and IT resource groups.

C1: Discuss three recommendations for role-based access controls that can be configured in alignment with the principle of least privilege based on the business requirements in the given scenario.

1. Ensure Key Vaults to Resource Group Allocation:
   - Ensure all Key Vaults are assigned to the correct resource group. If any Key Vaults are assigned to the incorrect resource groups, fix by assigning them to the correct resource group.
   - This recommendation aims to align with the principle of least privilege by restricting access to Key Vaults based on resource group allocation, ensuring that users only have access to Key Vaults within their designated resource groups.
2. Department-Specific Key Vault Contributors:
   - Assign the role of Key Vault Contributor at the department level to ensure that users within each department have the necessary permissions to manage Key Vaults but only for their specific department.
   - This aligns with the principle of least privilege by granting permissions only to those users who require access to the Key Vault for their specific department. Users from one department won't have unnecessary access to Key Vaults associated with other departments.
3. Tag Management for Departmental Resources:
   - Assign users from each department the role of Tag Contributor to allow them to manage tags for resources within their respective resource groups.
   - This aligns with the principle of least privilege by enabling departmental users to manage tags for their specific resources without giving them broader permissions. It allows for efficient resource organization and identification.

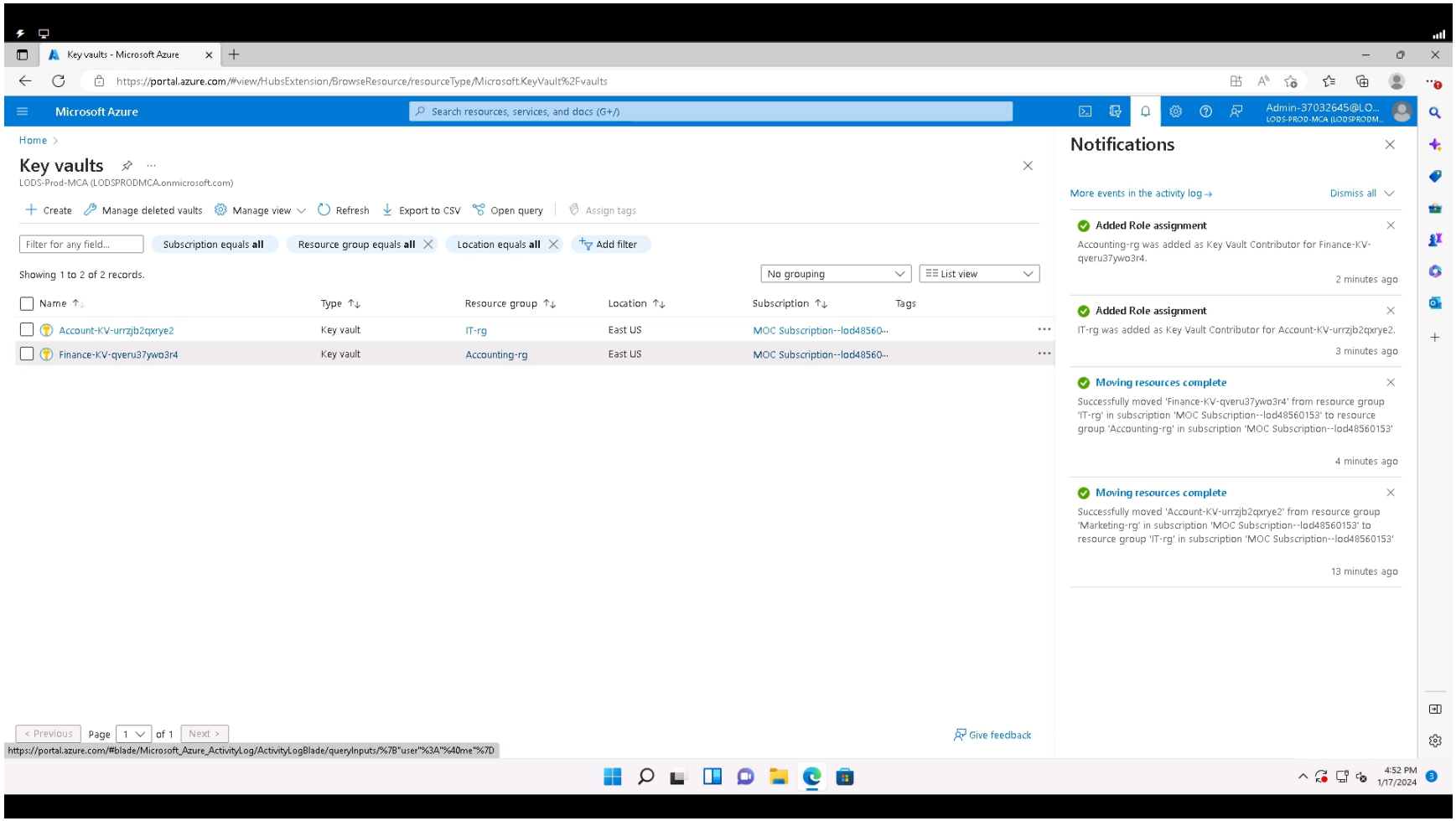
C2: Configure the role-based access controls in alignment with your given recommendations in part C1 and provide a screenshot for each of the updated configurations. The screenshots must be clear and show the full view of your screen, including the date and time.

1. Ensure Key Vaults to Resource Group Allocation:



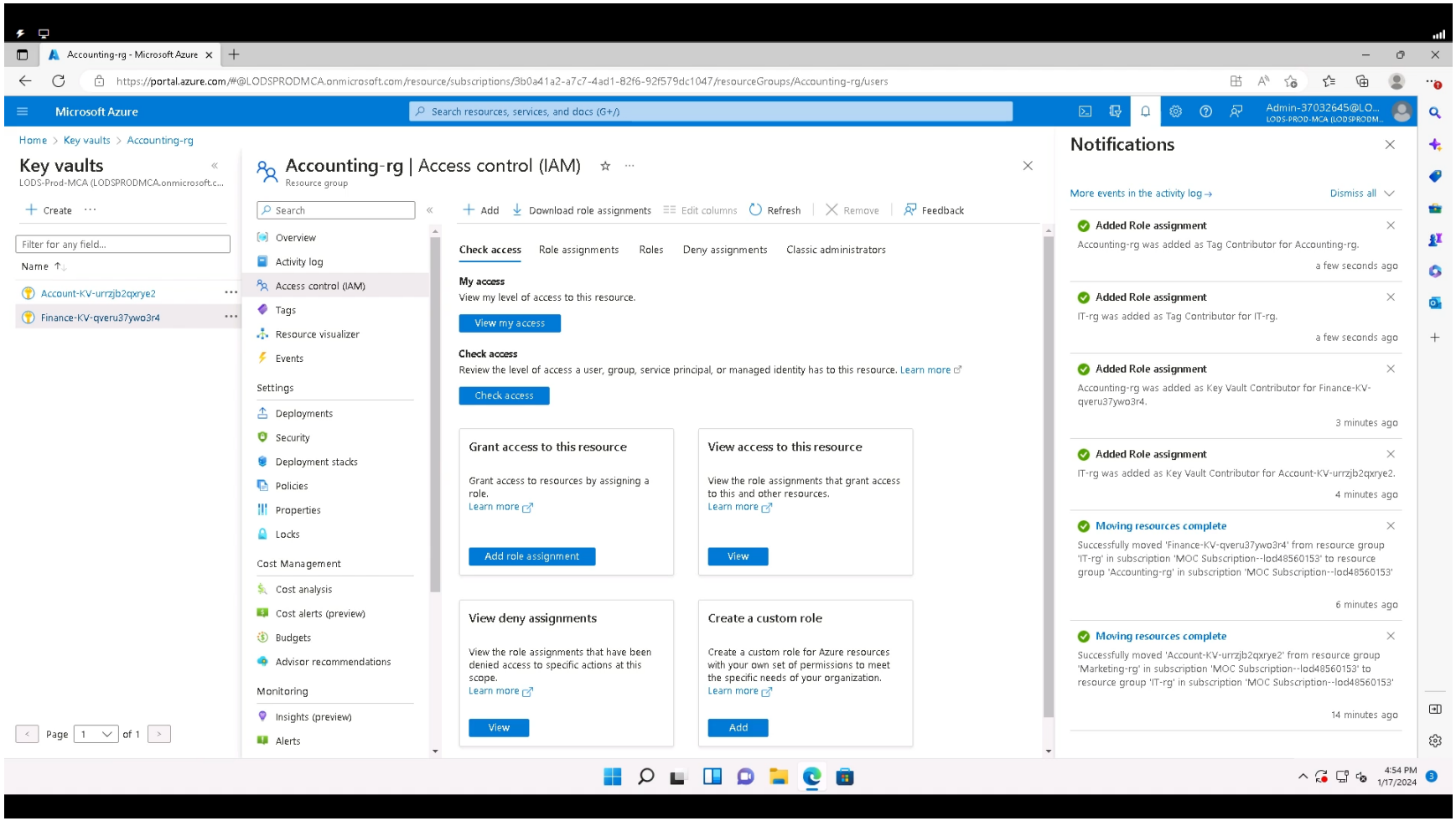
(Screenshot of lab showing that the Key Vaults are now allocated to the correct Resource Groups)

2. Department-Specific Key Vault Contributors:



(Screenshot of lab showing that the role of Key Vault Contributor has been added for the Key Vaults; shown in Notifications Tab)

3. Tag Management for Departmental Resources:

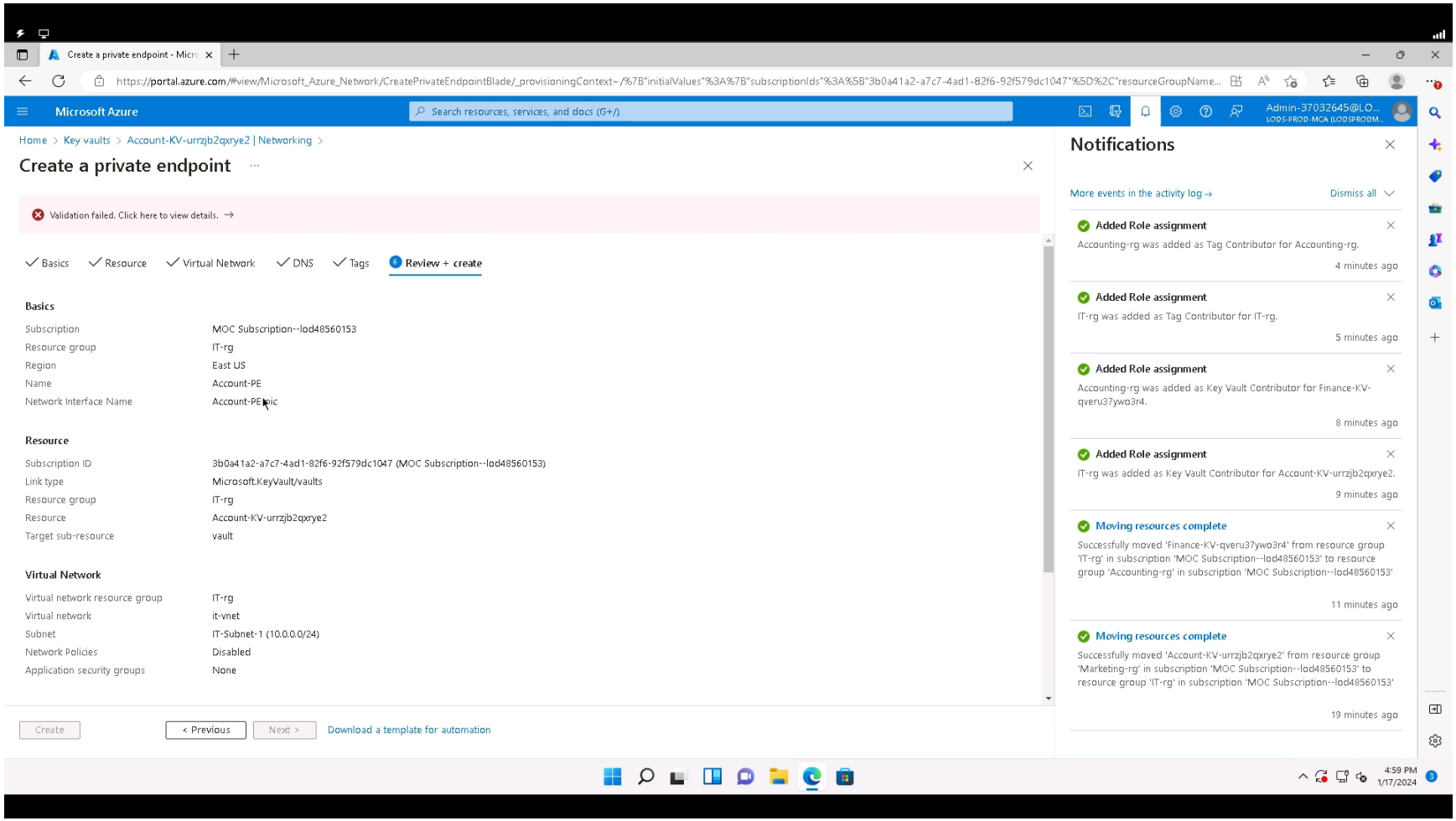


(Screenshot of lab showing that the role of Tag Contributor has been added for the Resource Groups; shown in Notifications Tab)

D: Analyze the existing Azure Key Vaults in the cloud lab environment focusing on encrypting data in transit and data at rest for the marketing, accounting, and IT resource groups.

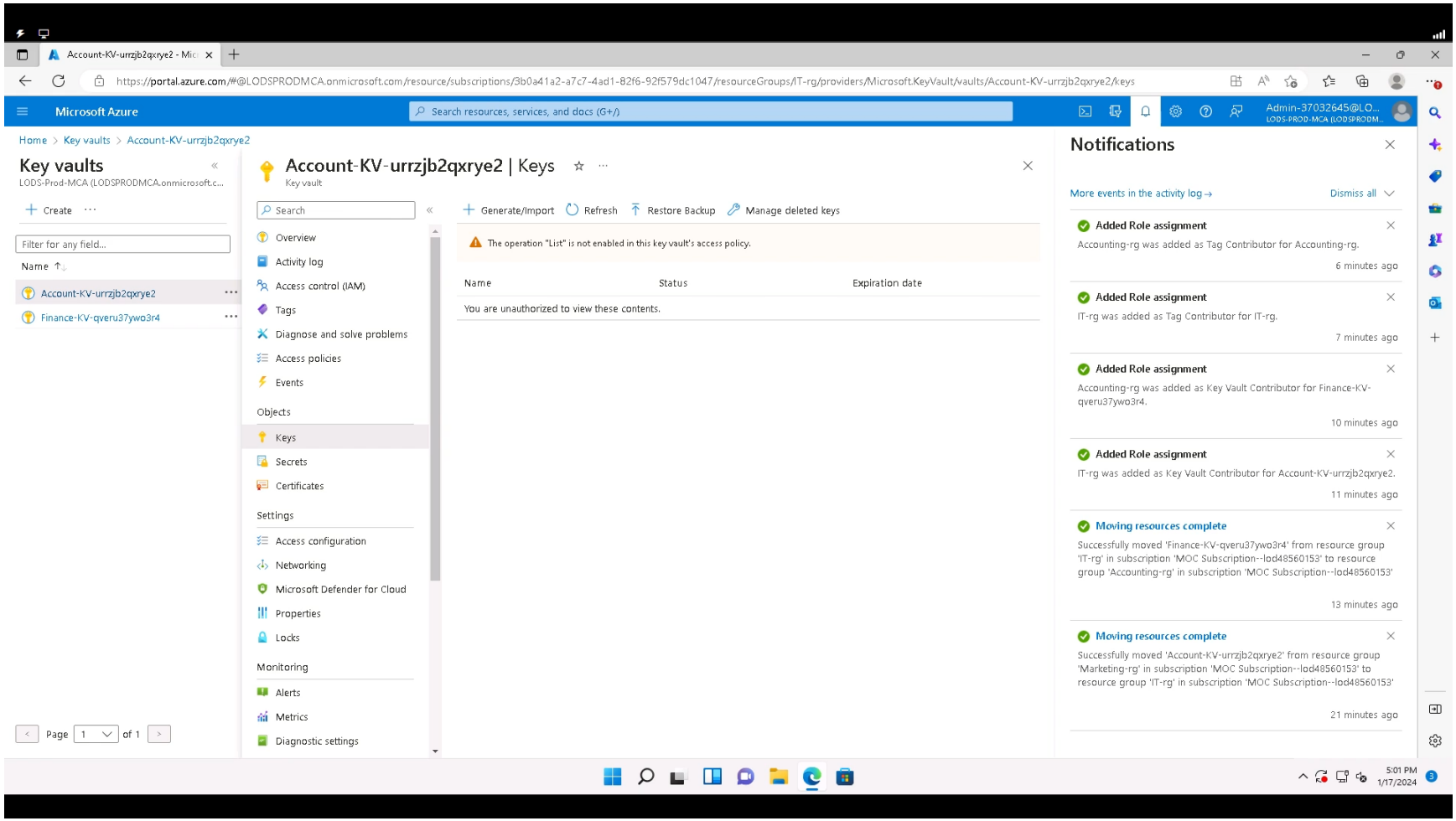
D1: Implement two best practices for Azure Key Vaults applicable to the resource groups listed and in alignment with the given scenario, providing screenshots of your updated access policies for each group. The screenshots must be clear and show the full view of your screen, including the date and time.

1. Implementing Private Endpoints for Key Vaults:



(Screenshot of lab showing the attempted creation of a Private Endpoint; unable to complete due to lab restrictions)

2. Implementing Key Rotation and Versioning:



(Screenshot of lab showing the attempted implementation and versioning of Keys; unable to complete due to lab restrictions)

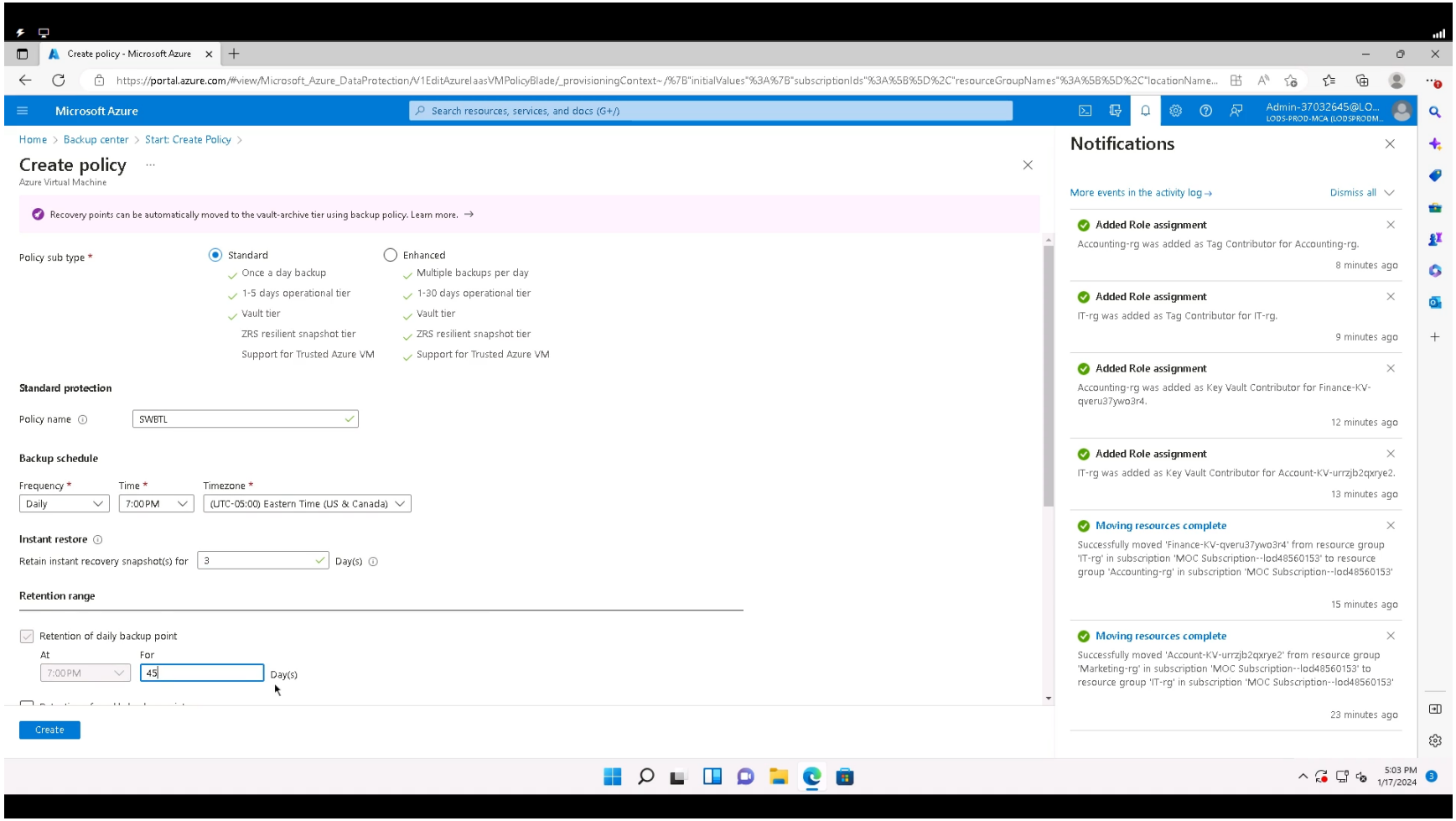
D2: Explain two recommendations for how the key vaults can be used to encrypt both data at rest and data in transit.

1. Service Endpoint with Azure Private Link:
    - Azure Private Link allows you to access Azure Key Vaults over a private, dedicated connection rather than over the public internet. By associating Key Vaults with a private endpoint in a Virtual Network, you establish a secure communication channel within the Microsoft backbone network. This ensures that data in transit between your applications and Key Vaults remains within the Azure network, reducing exposure to potential threats on the public internet. Private Link provides a more controlled and isolated environment for data exchange, enhancing security.
2. TLS/SSL Encryption for Key Vault Communication:
    - Enabling TLS/SSL encryption for communication between your applications and Azure Key Vaults ensures the confidentiality and integrity of data during transit. This encryption protocol establishes a secure, encrypted channel, preventing unauthorized parties from intercepting or tampering with sensitive information. TLS/SSL encryption is a standard security measure used to protect data in transit over the network. It involves the use of certificates to authenticate the Key Vault and encrypt the communication, making it resistant to eavesdropping and man-in-the-middle attacks.

E: Analyze the current state of file backups in the cloud lab environment for the company.

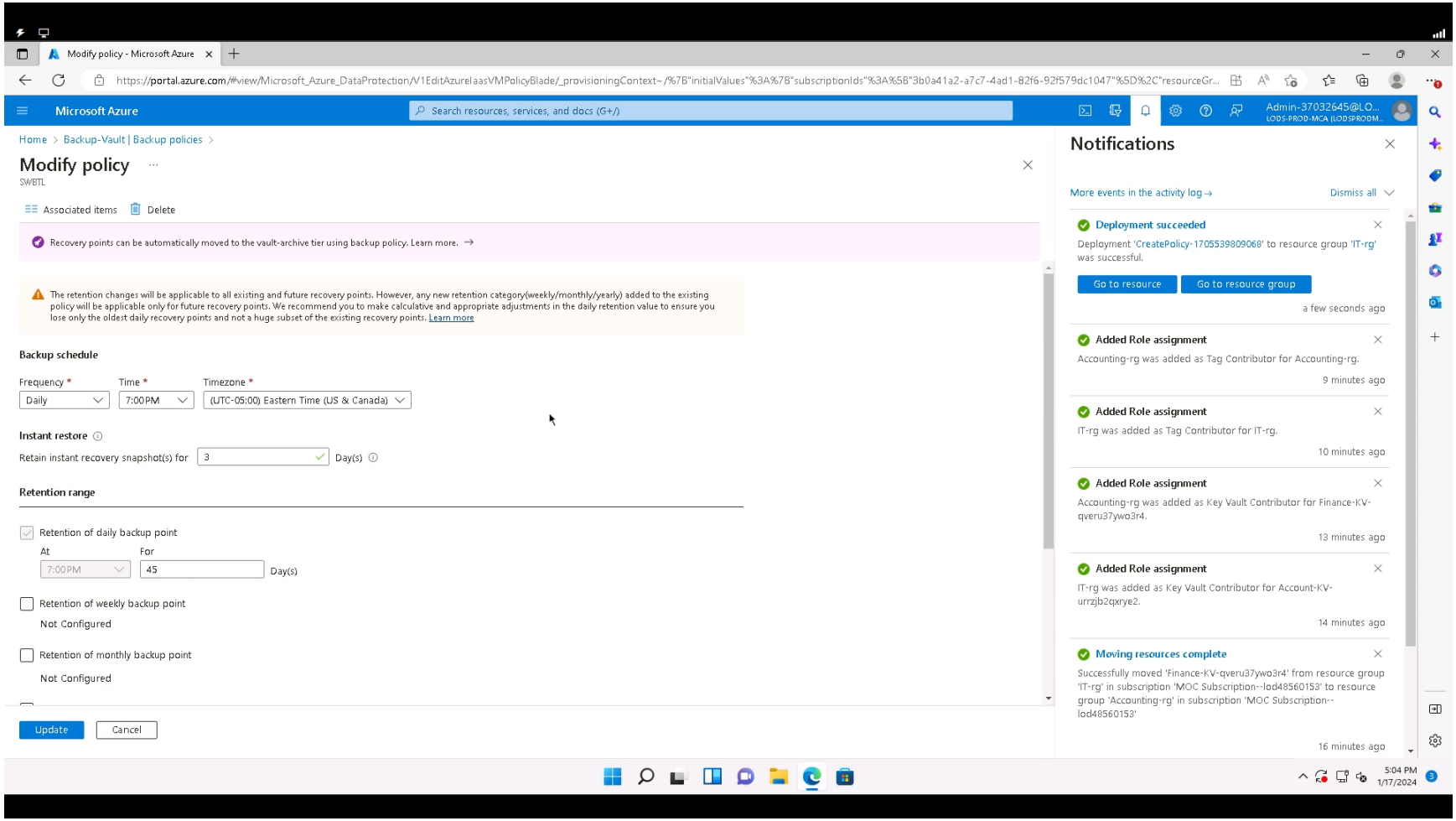
E1: Configure two settings for file backups that are in alignment with the given scenario, providing screenshots of your updated configurations. The screenshots must be clear and show the full view of your screen, including the date and time.

1. Backup Policy Configuration:



(Screenshot of lab showing the creation of a new Backup Policy)

2. Retention Settings for File Backups:



(Screenshot of lab showing the modification of Backup Policy to align Retention Settings with Business Requirements)

E2: Explain how the updated configurations from part E1 support the business requirements.

1. Backup Policy Configuration:
   - The configuration of a new backup policy named "SWBTL" aligns with the business requirement by ensuring that specific backup configurations are applied uniformly to the virtual machines. This policy allows for a standardized and organized approach to file backups, ensuring that each file backup instance follows the defined policies.
2. Retention Settings for File Backups:
   - Adjusting the retention settings for file backups ensures that daily backup points are retained for a duration that aligns with the company's recovery time objective (RTO) of 36 hours. This configuration facilitates the ability to restore files to a specific point within the required timeframe, meeting the business continuity objectives.

F: Describe the division of security responsibilities between the company and the cloud service provider (Azure), including shared responsibilities if any, for the cloud service model you selected in part B.

1. Company Responsibilities:
   - Data Protection and Access Control:
     - The company is responsible for protecting its data and defining access controls. This includes encrypting sensitive data, managing encryption keys, and determining who has access to what resources within the virtual infrastructure.
   - Operating System and Application Security:
     - Security measures within the virtual machines (VMs), including the operating system and applications running on them, are the responsibility of the company. This involves applying security patches, configuring firewalls, and implementing security best practices for the OS and applications.
   - Network Security:
     - Configuring and managing network security, such as setting up virtual networks, subnets, and network security groups, falls under the company's responsibility. This includes defining and enforcing network access controls and implementing security groups to restrict traffic.
   - Identity and Access Management (IAM):
     - The company is responsible for managing user identities, defining roles and permissions, and implementing access controls. This involves using identity services like Azure Active Directory to ensure secure authentication and authorization.
   - Application Security:
     - Securing the custom applications deployed on IaaS is the responsibility of the company. This includes code security, API security, and ensuring that applications are configured securely to prevent vulnerabilities.
2. Azure Responsibilities:
   - Physical Infrastructure Security:
     - Azure is responsible for the physical security of the underlying infrastructure, including data centers, servers, and networking equipment. This involves implementing measures to prevent unauthorized access to the physical hardware.

- Hypervisor and Virtualization Security:
  - Azure manages the security of the hypervisor and virtualization layer. This includes ensuring the isolation and security of virtual machines running on shared hardware.
- Network Infrastructure Security:
  - Azure is responsible for the security of the underlying network infrastructure, including the global network that connects data centers. This involves implementing measures to protect against DDoS attacks and other network threats.
- Data Center and Facility Security:
  - Azure is responsible for securing the data centers and facilities where the IaaS resources are hosted. This includes physical security measures, environmental controls, and compliance with industry standards.
- Managed Services Security:
  - Azure manages the security of its own services, such as Azure Key Vault, Azure Active Directory, and other platform services. This includes ensuring the security and availability of these services.

3. Shared Responsibilities:
   - Security of the Cloud:
     - Both the company and Azure share the responsibility for the overall security of the cloud infrastructure. This includes collaboration to protect against common security threats and vulnerabilities.
   - Compliance and Regulatory Requirements:
     - Meeting compliance standards and regulatory requirements is a shared responsibility. Azure provides a secure platform, and the company is responsible for configuring and using services in compliance with relevant regulations.
   - Incident Response and Monitoring:
     - Detecting and responding to security incidents is a shared responsibility. Azure provides monitoring tools, and the company is responsible for configuring and actively monitoring its resources.

F1: Discuss three risks assumed by the company for the cloud service model based on the shared responsibilities identified in part F, and include in your discussion the level of impact each risk may have on the company's use of cloud computing resources.

1. Data Security:
   - The company bears the responsibility for securing data within its virtual machines and applications. This includes implementing encryption measures for data at rest and in transit, aligning with industry standards and regulatory requirements.
2. Access Controls:
   - Role-Based Access Controls (RBAC) configuration and management fall under the company's purview. Ensuring least privilege access and conducting regular audits to align with changing organizational structures are company responsibilities.
3. Backup and Recovery:
   - The IT department is accountable for performing and verifying backups, establishing recovery objectives, and maintaining backup policies. This includes managing recovery point objectives (RPO) and recovery time objectives (RTO) to meet business continuity needs.

F2: Explain three recommendations to ensure compliance with the company's cloud security posture, and include a justification based on industry best practices for each recommendation.

1. Continuous Monitoring:
   - Implement continuous monitoring practices to ensure that security configurations and access controls are consistently aligned with the company's security policies. Utilize Azure monitoring tools to detect and respond to security events promptly.
2. Regular Audits:
   - Conduct regular audits of Azure configurations and access controls to identify and rectify any deviations from the established security posture. Regular reviews help in maintaining compliance and minimizing the risk of security misalignments.
3. Security Training:
   - Provide ongoing training for IT administrators and relevant staff to stay updated on the latest Azure security features and best practices. Well-informed personnel contribute to a more secure cloud environment.

G: Explain three threats that have the potential to impact the company's updated cloud solution, and include in the explanation the threat mitigation countermeasures that could be used to minimize the impact of each threat.

1. Unauthorized Access:
   - Threat Description:
     - Unauthorized access poses a significant risk, especially considering the reported data visibility across teams. If not addressed, it could lead to data breaches, compromising sensitive information.
   - Mitigation Countermeasures:
     1. Implement Multi-Factor Authentication (MFA) for all user accounts to add an additional layer of security.
     2. Regularly audit and update Role-Based Access Controls (RBAC) to align with the principle of least privilege.
     3. Utilize Azure Active Directory Identity Protection to detect and respond to risky sign-ins promptly.
2. Data Breach due to Insufficient Encryption:
   - Threat Description:
     - Inadequate encryption measures for data at rest and in transit could expose sensitive information, violating regulatory requirements and jeopardizing data integrity.
   - Mitigation Countermeasures:
     1. Enforce Azure Disk Encryption for virtual machines to protect data at rest.
     2. Utilize Azure Key Vault for centralized management of encryption keys.
     3. Implement Azure Virtual Network Service Endpoints to secure data in transit.
3. Backup and Recovery Failures:
   - Threat Description:
     - Incomplete or failed backups could jeopardize the company's ability to recover critical data in the event of a disaster, leading to prolonged downtime and potential data loss.
   - Mitigation Countermeasures:
     1. Regularly test backup and recovery processes to ensure they meet the Recovery Point Objective (RPO) and Recovery Time Objective (RTO).
     2. Utilize Azure Backup for automated and reliable backup solutions.
     3. Implement geo-redundancy for backup storage to enhance data resilience and availability.

I: Acknowledge sources, using in-text citations and references, for content that is quoted, paraphrased, or summarized.

Chapple, M., & Seidl, M. (2023). (ISC)2 CCSP certified cloud security professional official study guide. Sybex. (3rd ed.) https://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=3375845&site=eds-live&scope=site

Copeland, M., Soh, J., Puca, A., & Harris, M. (2020). Microsoft Azure: Planning, Deploying, and Managing the Cloud. (2nd Edition). Springer. https://wgu.percipio.com/books/3066d572-95c9-49c4-ac7d-9a3c35458b25#epubcfi(/6/4!/4/2[epubmain]/2[g4b3ab31c-3312-43db-ab7d-aa8b2115ff18]/2/2/1:0)

Estrin, E. (2022). Cloud security handbook: Find out how to effectively secure cloud environments using AWS, Azure, and GCP. Packt Publishing. https://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=3198558&site=eds-live&scope=site

National Institute of Standards and Technology. (n.d.). NIST cybersecurity framework (CSF). https://www.nist.gov/cyberframework