

# **Cloud Security Implementation Plan**

Jamal Rizki

## **SWBLT LLC Cloud Migration**

### **A. Executive Summary**

SWBTL LLC began as a small regional delivery service provider and has since evolved into a nationwide service provider with over 2,000 employees. The company's infrastructure is currently hosted in four data centers located in the United States. Over time these systems have become increasingly costly, as SWBTL does not own the data centers and is instead leasing them from a third party. Other concerns the company currently faces include an unreliable service and a threat surface potentially vulnerable to cyberattacks. The company must also comply with FISMA and PCI DSS regulations and has a NIST SP 800-53 audit approaching. Due to these factors, the company has decided to transition to the cloud. To begin this transition, the company will focus on the Marketing, Accounting, and IT departments, using Microsoft Azure as the service provider.

### **B. Proposed Course of Action**

To best meet SWBTL LLC's requirements, the implementation of an Infrastructure as a Service (IaaS) model is the best course of action. This is due to the company's need to deploy and manage virtual machines and

operating systems, provision compute and storage resources, and integrate custom applications.

Regulatory compliance requirements include adhering to FISMA for government contracts, PCI DSS for the processing of credit card data, and NIST SP 800-53 guidance controls for the upcoming assessment. Microsoft Azure allows SWBTL to scale rapidly, it also reduces the associated costs by provisioning only the minimum resources required, and it also integrates seamlessly with the existing Active Directory configuration the company uses. In addition, Azure offers strong encryption services for both data in transit and at rest, as well as the management of passwords, credentials, and secrets through Azure Key Vault. Challenges to this migration include the complex process of transferring large volumes of data, ensuring that data remains secure and is accessible only to authorized parties, and establishing suitable backup and recovery processes to minimize risks at all stages of the migration and beyond.

## **C1. Analysis and Recommendations**

Currently the role-based access controls at SWBTL are not aligning with the principles of least privilege best practices. There are many configurations where the roles are set to be broader than necessary.

Three recommendations to address these flaws are:

1. Assign roles based on departmental function – Assigning basic Reader permissions to departments that only interact with the resources at a low level. The Marketing and Accounting departments should be restricted from altering resources to avoid accidental or intentional changes.
2. Implement least privilege across departments - Each department should be isolated from the others to avoid unauthorized access to or altering of another department's resources.
3. Remove unnecessary management or subscription-level access - Default permissions at the subscription or administrative level could allow users to bypass departmental boundaries.

## **C2. Updated Configurations**



Accounting – The Accounting security group was assigned the role of Reader. This provides visibility of resources without allowing any modifications.

Microsoft Azure | Search resources, services, and docs (G+)

Home > Accounting-rg | Access control (IAM)

### Add role assignment

Role: **Members** | Conditions | Assignment type | Review + assign

Showing a filtered list of roles because your permissions include a condition. [Learn more](#)  
[View my access](#)

**Selected role**: Reader

**Assign access to**:  User, group, or service principal  
 Managed identity

**Members**: + Select members

Name	Object ID	Type
No members selected		

**Description**: Optional

Buttons: Review + assign, Previous, Next, Select, Close

Selected members: Accounting Security Group for Accounting

Home > Accounting-rg | Access control (IAM)

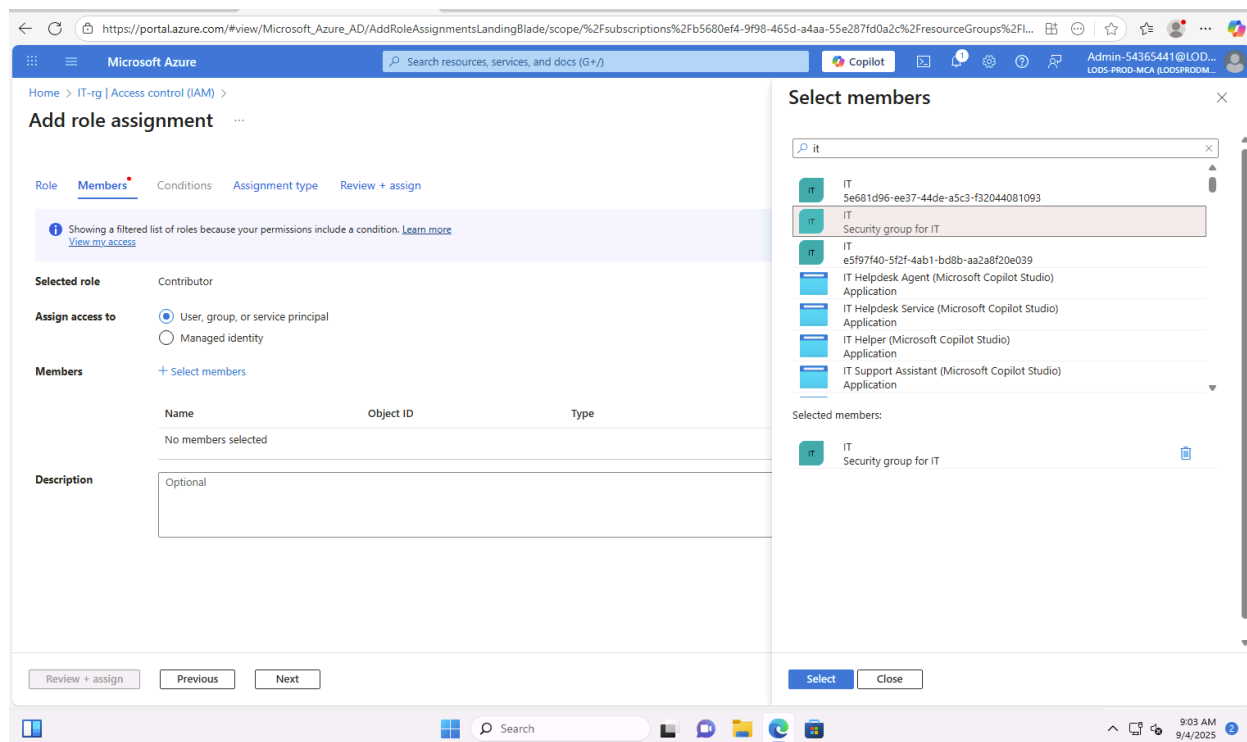
Search: [ ]

Buttons: Add, Download role assignments, Edit columns, Refresh, Delete, Feedback

Role	Member	Member Type	Assignment Type	Start Date	End Date	Permissions
Contributor (1)	cloud-slice-app	Service principal	Owner	Active	Permanent	Permanent
	cloud-slice-app	Service principal	Owner	Active	Permanent	Permanent
	cloud-slice-app	Service principal	Owner	Active	Permanent	Permanent
	cloud-slice-app	Service principal	Owner	Active	Permanent	Permanent
	cloud-slice-app	Service principal	Owner	Active	Permanent	Permanent
	cloud-slice-app	Service principal	Owner	Active	Permanent	Permanent
Reader (3)	Accounting	Group	Reader	Active	Permanent	Permanent
	LODS Readers	Group	Reader	Active	Permanent	Permanent
	Wiz for Azure	Service principal	Reader	Active	Permanent	Permanent
Azure Kubernetes Service Cluster User Role (1)	Wiz for Azure	Service principal	Azure Kubernetes Servic...	Active	Permanent	Permanent
	Wiz for Azure	Service principal	Azure Kubernetes Servic...	Active	Permanent	Permanent
Azure Kubernetes Service RBAC Reader (1)	Wiz for Azure	Service principal	Azure Kubernetes Servic...	Active	Permanent	Permanent

URL: https://portal.azure.com/#using...  
Time: 9:00 AM 9/4/2025

IT– The IT security group was assigned the role of Contributor. This allows changes and modifications to resources but not permissions to assign or alter roles.



The screenshot displays the Microsoft Azure portal interface for adding a role assignment. The main pane shows the 'Add role assignment' wizard with the following details:

- Role:** Contributor
- Assign access to:** User, group, or service principal (selected)
- Members:** No members selected
- Description:** Optional

The 'Select members' pane is open on the right, showing a search for 'it' and a list of IT-related groups. The 'IT Security group for IT' is selected.

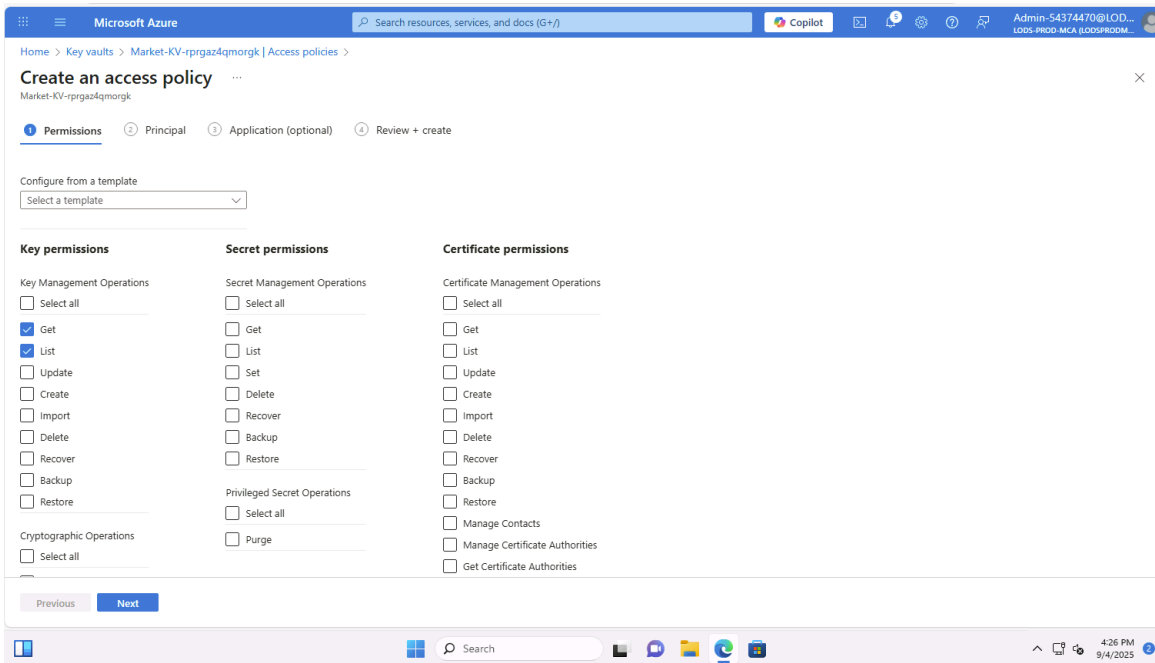
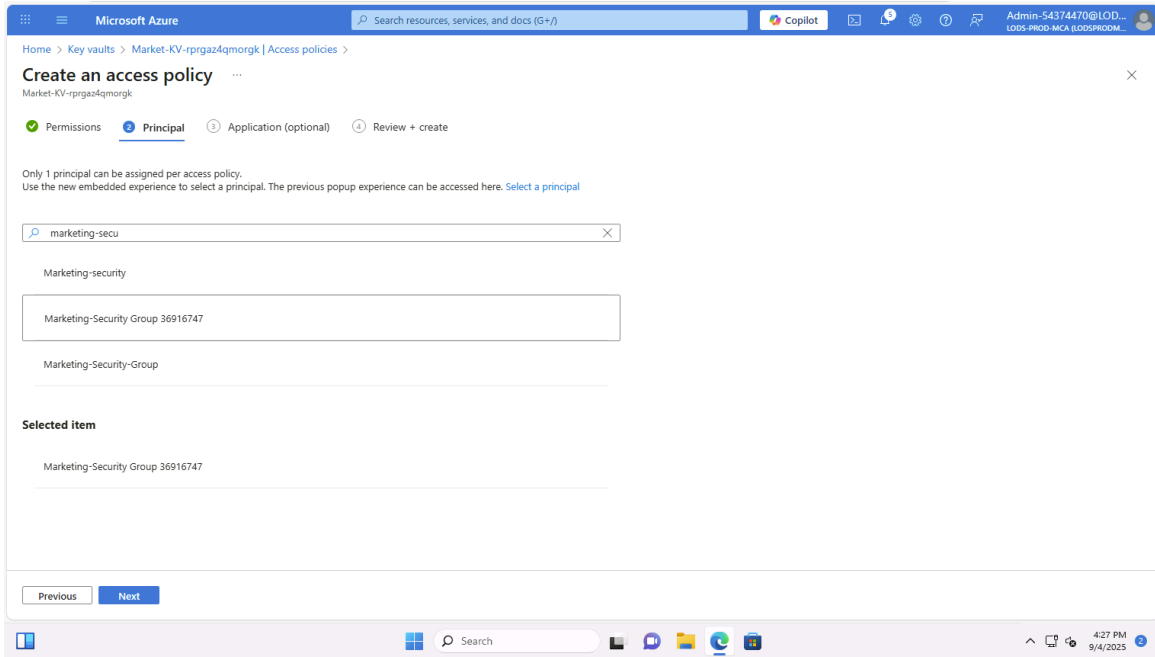
Name	Object ID	Type
No members selected		

The 'Select members' pane shows the following list of members:

- IT Security group for IT (Selected)
- IT Helpdesk Agent (Microsoft Copilot Studio) Application
- IT Helpdesk Service (Microsoft Copilot Studio) Application
- IT Helper (Microsoft Copilot Studio) Application
- IT Support Assistant (Microsoft Copilot Studio) Application

The bottom of the screen shows the Windows taskbar with the time 9:03 AM on 9/4/2025.





This screenshot shows the 'Access policies' configuration page for the key vault 'Market-KV-rprgaz4qmorgk'. The left sidebar contains a navigation menu with options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Access policies (selected), Resource visualizer, Events, Objects, Settings, Monitoring, Automation, and Help. The main content area shows a search bar, a '+ Create' button, and a table of access policies. The table has columns for Name, Email, Key Permissions, Secret Permissions, and Certificate Permissions. One policy is listed under the 'GROUP' section: 'Marketing-Security Group...' with 'Get, List' permissions. The top navigation bar includes the Microsoft Azure logo, a search bar, Copilot, and the user profile 'Admin-54374470@LOD...'. The bottom taskbar shows the Windows Start button, search bar, and system tray with the time '4:27 PM 9/4/2025'.

This screenshot shows the 'Networking' configuration page for the key vault 'Market-KV-rprgaz4qmorgk'. The left sidebar navigation menu is similar to the previous screenshot but includes 'Access configuration' and 'Networking' (selected). The main content area is divided into 'Firewalls and virtual networks' and 'Private endpoint connections'. Under 'Firewalls and virtual networks', there are sections for 'Allow access from:' with radio buttons for 'Allow public access from all networks', 'Allow public access from specific virtual networks and IP addresses' (selected), and 'Disable public access'. Below this is the 'Virtual networks' section, which includes a table with columns for Virtual network, Subnet, Address Range, Endpoint Status, Resource group, and Subscription. The table is currently empty with the text 'No virtual networks are selected.'. There are also sections for 'Firewall' (to add IP ranges) and 'Exception' (to add client IP addresses). The top navigation bar and bottom taskbar are consistent with the previous screenshot, showing the time '4:11 PM 9/4/2025'.

# Finance resource group:

Microsoft Azure | Search resources, services, and docs (G+)

Home > Key vaults > Finance-KV-k54fk6qoenug | Access policies >

## Create an access policy

Finance-KV-k54fk6qoenug

Permissions **Principal** Application (optional) Review + create

Configure from a template  
Select a template

Key permissions	Secret permissions	Certificate permissions
<input type="checkbox"/> Select all	<input type="checkbox"/> Select all	<input type="checkbox"/> Select all
<input checked="" type="checkbox"/> Get	<input type="checkbox"/> Get	<input type="checkbox"/> Get
<input checked="" type="checkbox"/> List	<input type="checkbox"/> List	<input type="checkbox"/> List
<input type="checkbox"/> Update	<input type="checkbox"/> Set	<input type="checkbox"/> Update
<input type="checkbox"/> Create	<input type="checkbox"/> Delete	<input type="checkbox"/> Create
<input type="checkbox"/> Import	<input type="checkbox"/> Recover	<input type="checkbox"/> Import
<input type="checkbox"/> Delete	<input type="checkbox"/> Backup	<input type="checkbox"/> Delete
<input type="checkbox"/> Recover	<input type="checkbox"/> Restore	<input type="checkbox"/> Recover
<input type="checkbox"/> Backup		<input type="checkbox"/> Backup
<input type="checkbox"/> Restore		<input type="checkbox"/> Restore
	Privileged Secret Operations	<input type="checkbox"/> Manage Contacts
	<input type="checkbox"/> Select all	<input type="checkbox"/> Manage Certificate Authorities
	<input type="checkbox"/> Purge	<input type="checkbox"/> Get Certificate Authorities
Cryptographic Operations		
<input type="checkbox"/> Select all		

Previous **Next**

Microsoft Azure | Search resources, services, and docs (G+)

Home > Key vaults > Finance-KV-k54fk6qoenug | Access policies >

## Create an access policy

Finance-KV-k54fk6qoenug

Permissions **Principal** Application (optional) Review + create

Only 1 principal can be assigned per access policy.  
Use the new embedded experience to select a principal. The previous popup experience can be accessed here. [Select a principal](#)

accounting-sec

Accounting-security

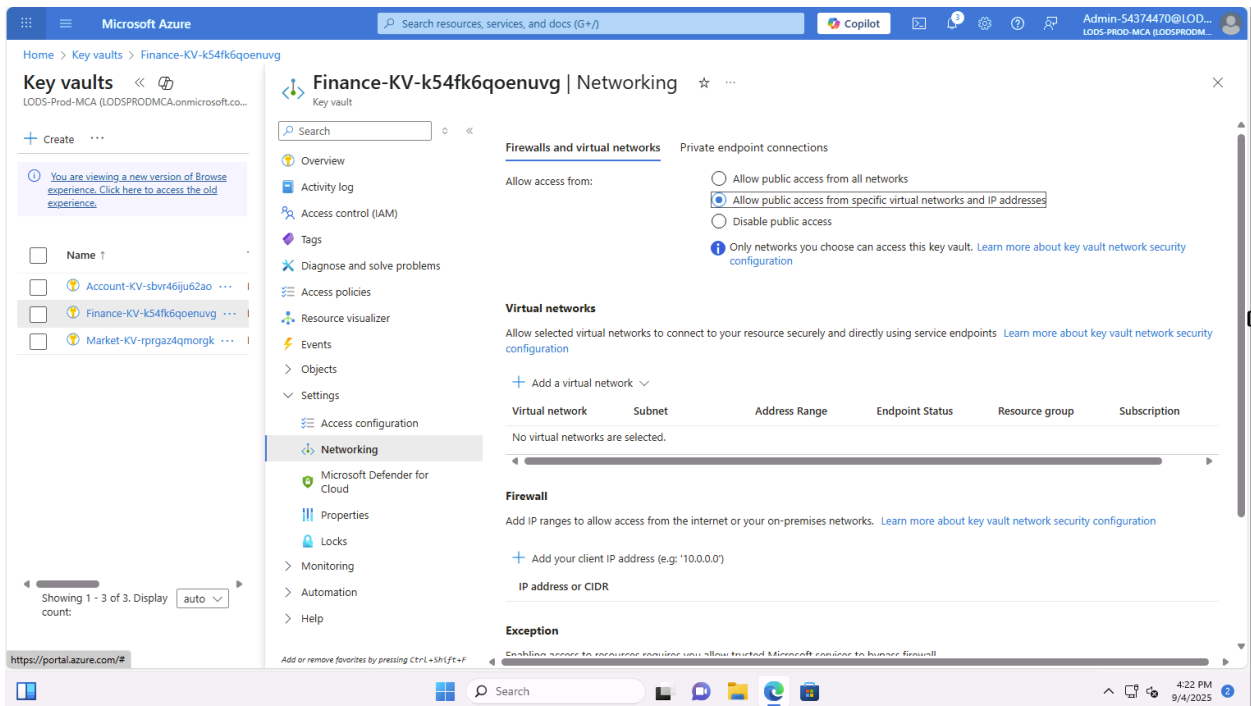
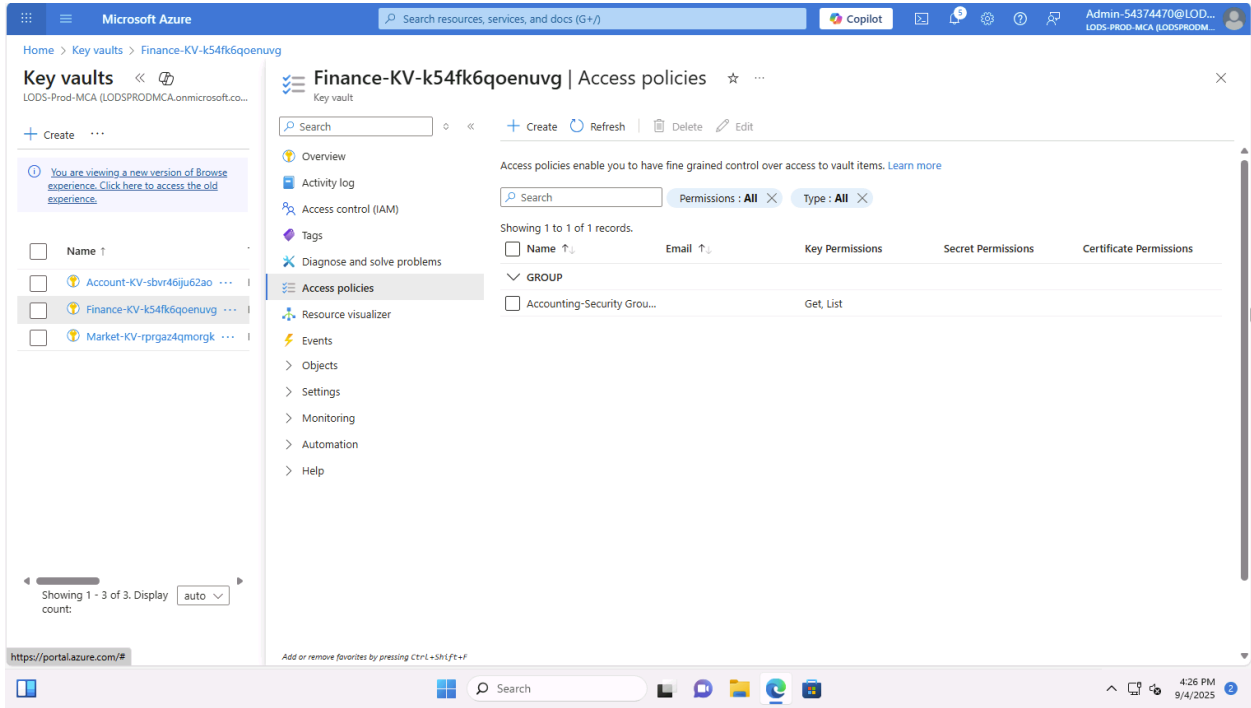
Accounting-Security Group 36916747

Accounting-Security-Group

**Selected item**

Accounting-Security Group 36916747

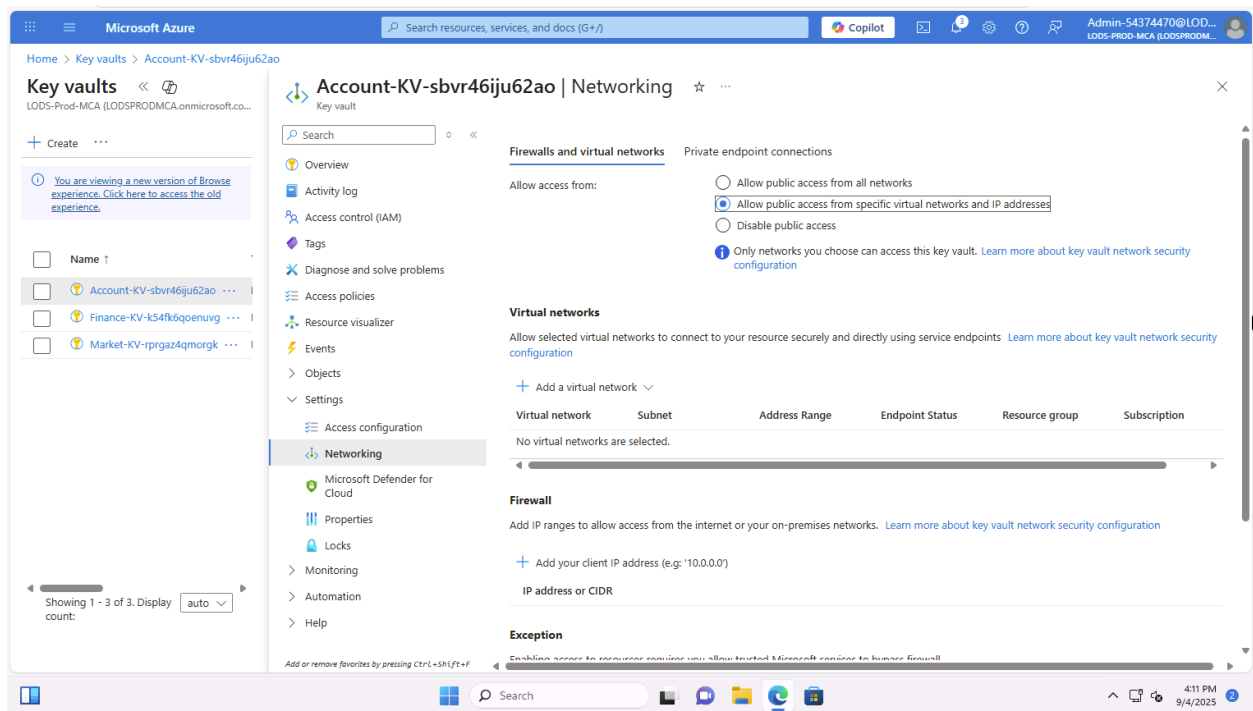
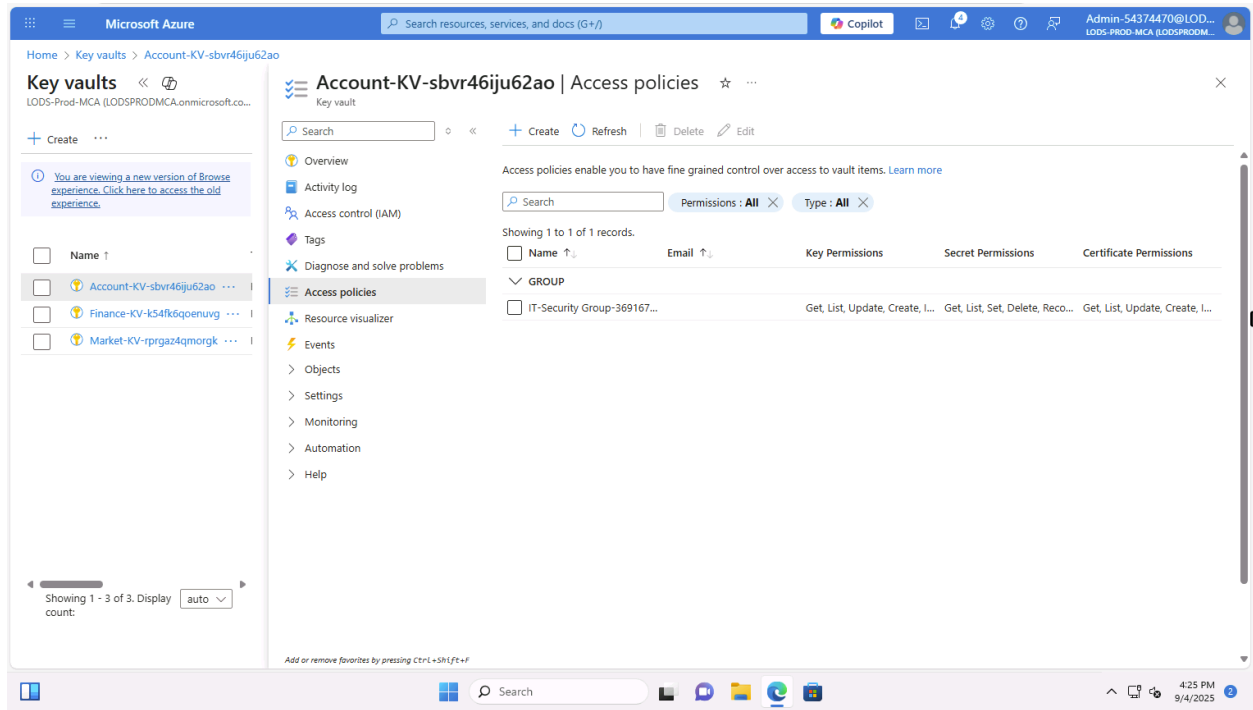
Previous **Next**



IT resource group:

This screenshot shows the 'Create an access policy' page in the Microsoft Azure portal. The page is titled 'Create an access policy' and is located under 'Home > Key vaults > Account-KV-sbvr46iju62ao | Access policies >'. The current step is 'Permissions', indicated by a blue circle with the number 1. The breadcrumb trail is 'Home > Key vaults > Account-KV-sbvr46iju62ao | Access policies >'. Below the breadcrumb, there are four steps: 1. Permissions (active), 2. Principal, 3. Application (optional), and 4. Review + create. A dropdown menu for 'Configure from a template' is set to 'Key, Secret, & Certificate Management'. The page is divided into three columns of permissions: 'Key permissions', 'Secret permissions', and 'Certificate permissions'. Each column has a 'Select all' checkbox and a list of specific operations with checkboxes. Under 'Key permissions', 'Cryptographic Operations' has a 'Select all' checkbox. At the bottom, there are 'Previous' and 'Next' buttons. The browser address bar shows 'https://portal.azure.com/#'. The Windows taskbar at the bottom shows the time as 4:24 PM on 9/4/2025.

This screenshot shows the 'Create an access policy' page in the Microsoft Azure portal, now on the 'Principal' step. The page title is 'Create an access policy'. The breadcrumb trail is 'Home > Key vaults > Account-KV-sbvr46iju62ao | Access policies >'. The current step is 'Principal', indicated by a blue circle with the number 2. The breadcrumb trail is 'Home > Key vaults > Account-KV-sbvr46iju62ao | Access policies >'. Below the breadcrumb, there are four steps: 1. Permissions, 2. Principal (active), 3. Application (optional), and 4. Review + create. A message states: 'Only 1 principal can be assigned per access policy. Use the new embedded experience to select a principal. The previous popup experience can be accessed here. [Select a principal](#)'. Below the message is a search box containing 'IT-sec'. A list of search results is shown: 'IT-security', 'IT-Security Group-36916747', and 'IT-Security-Group'. The 'Selected item' section shows 'IT-Security Group-36916747'. At the bottom, there are 'Previous' and 'Next' buttons. The browser address bar shows 'https://portal.azure.com/#'. The Windows taskbar at the bottom shows the time as 4:24 PM on 9/4/2025.



## D2. Encryption Recommendations

Data at rest – Azure Key Vaults can store and manage encryption keys, secrets, and certificates for services such as Storage Blobs, Databases, and Virtual Machines. The use of Key Vault ensures sensitive data is kept secure and also helps the company meet compliance goals.

Data in transit – Azure Key Vault can store and manage SSL/TLS certificates. This protects data in transit by preventing it from being intercepted or tampered with during communication between applications and services.

## **E1. Azure Cloud Backups**

I configured two different backup settings in the IT-rg Resource group including:

Virtual machine backup:

- Created a new policy named SWBTL
- Configured a daily backup at 7:00 PM EST.
- The backup retention period is set for 45-days
- Instant restore is set to 3 days

**Configure backup**

Policy sub type \*  Enhanced

- Multiple backups per day
- Up to 30 days operational tier retention
- Support for Trusted Launch Azure VM
- Support for VMs with Ultra Disks and Premium SSD v2

Backup policy \*  [Edit this policy](#)

**Policy details**

**Full backup**  
Daily at 7:00 PM Eastern Standard Time

**Instant restore**  
Retain instant recovery snapshot(s) for 3 day(s)

**Retention of daily backup point**  
Retain backup taken every day at 7:00 PM for 45 Day(s)

Consistency type  Application or file-system consistent

**Virtual machines**

Name	Resource group
No virtual machines selected.	

[Enable backup](#) [Download a template for automation](#)

**Create policy**

Recovery points can be automatically moved to the vault-archive tier using backup policy. [Learn more.](#)

Policy name

**Backup schedule**

Frequency \*  Time \*  Timezone \*

**Instant restore**

Retain instant recovery snapshot(s) for  Day(s)

**Retention range**

- Retention of daily backup point  
At  For  Day(s)
- Retention of weekly backup point  
Not Configured
- Retention of monthly backup point  
Not Configured
- Retention of yearly backup point

[OK](#)

**Backup-Vault | Backup items**

Try our new Business Continuity Center for the at scale BCDR management of your resources protected across Azure Backup and Site Recovery.

Primary Region Secondary Region

BACKUP MANAGEMENT TYPE	BACKUP ITEM COUNT
Azure Virtual Machine	1
Azure Backup Agent	0
Azure Backup Server	0
DPM	0
Azure Storage (Azure Files)	0
SQL Database in Azure VM	0
SAP HANA in Azure VM	0
SQL Server in Azure VM (Snapshot backup)(Preview)	0
SAP ASE (Sybase) in Azure VM	0

### File Share Backup:

The second example demonstrates a file share backup:

- Scheduled a daily backup at 7:30 pm UTC time
- Set backup retention period for 30-days
- As no file shares are currently available in the environment, the configuration demonstrates how it would be implemented at a future date.

The screenshot displays the Microsoft Azure portal interface for configuring a backup. The main window is titled 'Configure backup' and shows the following details:

- Storage Account:** vmstoragee7kvrrowe62jq
- FileShares to Backup:** No File Shares selected
- Policy details:** Backup policy: (new) DailyPolicy-mf67zcr6
- Full backup:** Backup frequency: Daily at 7:30 PM UTC; Retention of daily backup point: Retain backup taken every day at 7:30 PM for 30 Day(s)

A 'Select file shares' dialog is open on the right, showing a search for file shares in the storage account. The dialog indicates that no file shares are currently available for backup.

## E2. Supporting Business Requirements

The backup configurations implemented support business requirements by strengthening disaster recovery and regulatory compliance. They also protect against data loss caused by intentional or

unintentional errors and safeguard the company from system failures. These align with the requirements of SWBTL, including a 45-day backup policy, RPO of one day with daily backups scheduled, and snapshots maintained for 3 days.

### **F1. Shared Responsibility**

With Infrastructure as a Service (IaaS), the cloud provider is responsible for securing the hosts, network, and datacenters, while the customer is responsible for managing the operating system, controls, applications, identity and access management (IAM) policies, data, and devices (Microsoft, n.d).

#### Applicable Risks

1. Broken access controls - Misconfigured access controls can allow unauthorized users to exfiltrate data or launch cyberattacks. This represents a high risk because it directly compromises the confidentiality and integrity of company data.
2. Data loss - Proper storage and backup policies are the responsibility of the company. The impact is high due to its effect on data availability in the event of downtime or data loss.

3. Compliance issues - Without the correct compliance measures, the company faces a medium to high impact if it fails to meet applicable regulatory standards.

### Recommendations

1. Strong IAM policies - Use MFA, Principles of least privilege and conditional access policies to prevent unauthorized access
2. Strong Backup policies - Schedule and assess backup policies regularly to ensure data security
3. Continuous monitoring - Use tools, manual and automated monitoring solutions to meet compliance needs. (Microsoft, n.d).

### **G. Cloud Threats and Mitigation Tactics**

Some potential threat vectors and migration tactics are:

1. Data Breaches – Misconfigurations can include weak access controls, flaws in software configurations, and unauthorized data exfiltration from storage accounts.
  - Mitigation countermeasures – This includes encryption of data, effective use of firewalls and IAM policies, and monitoring of suspicious behavior patterns.

2. Insider threats – Employees may intentionally or unintentionally cause system disruptions.
  - Mitigation countermeasures – Implementing robust access controls and maintaining the principle of least privilege best practices.
3. Account hijacking – If a bad actor compromises a user account it could lead to unauthorized access to data and resources.
  - Mitigation countermeasures – Adhering to granular access policies limits the attack surface should an account be compromised. Multifactor authentication can help prevent initial access.

## **References**

Microsoft. Shared responsibility in the cloud. (n.d.). Retrieved September 5, 2025, from <https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility>

Microsoft. Cloud adoption framework: Secure methodology in Azure. (n.d.). Retrieved September 5, 2025, from <https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/govern/monitor-cloud-governance>

