UDACITY

Data Security Analysis in Online Payment Processing

Hazrat Umer

19 Aug 2024

Project Scenario

Project Scenario

You have recently joined JFin Payments, a rapidly growing online payment processing firm based in Los Angeles, California, as a Data Security Analyst. With over 100,000 **customers across the United States and Europe**, JFin Payments handles a diverse range of sensitive data, including employee and customer profiles, financial information, company communications, and intellectual property.

As a key member of the data security team, your primary responsibility is to ensure the confidentiality, integrity, and availability of the company's data assets. To achieve this, you will collaborate with the data warehouse and application and infrastructure security teams to develop and implement robust data security policies, procedures, and controls.

Throughout the project, you will leverage your expertise in data security, regulatory compliance, and risk management to fortify JFin Payments' data security posture. Your insights and recommendations will play a crucial role in safeguarding sensitive information, maintaining customer trust, and supporting the company's continued growth in the competitive online payment processing industry.

Section One:
Data Governance

Strategic Data Security Policies

In the rapidly evolving digital landscape, the security of sensitive information remains a cornerstone of JFin Payments' operations. The diversity of data managed—from customer financial details to internal communications and intellectual property—presents a complex challenge in maintaining confidentiality, integrity, and availability. Your role involves contributing to the safeguarding of this information by understanding and evaluating the benefits of key data security program policies provided by the company.

- Review the policy items provided on the next slide.
- For each item, write a brief explanation of its benefits. Consider aspects such as data security, compliance, risk management, and operational efficiency.

Strategic Data Security Policies

IT Staff should perform a data classification annually, or when there are notable business or technology changes.
Annual data classification or when there are notable business or technology changes helps enhance security. Every sensitive piece of information is identified and can be secured to its level of criticality. This helps organizations apply the correct security controls and protects data from unauthorized access and breaches. It also helps organizations to remain compliant with industry regulations, benefits them in risk management, cost reduction, and better decision-making, and improves their security posture.
IT Staff should perform an application and critical system classification annually, or when there are notable business or technology changes.
Classifying applications and critical systems helps IT staff know which system or component in a business has the utmost importance to the organization. Through classification, they know about system or application criticality. After classification, they can decide which system or application contains critical data that should be secured first.
IT Staff should perform a regulatory assessment annually, or when there are notable business or technology changes.
Conducting annual regulatory assessments helps organizations remain compliant with the latest industry regulations. Being compliant will help them avoid penalties and the loss of customer trust. Through an annual regulatory assessment, the organization will know and address if there is any gap in being compliant with industry regulations and will keep its policies aligned with regulatory standards.

Data Classification

As a Data Security Analyst at JFin Payments, one of your primary responsibilities is to ensure the confidentiality, integrity, and availability of the company's data assets. To effectively protect sensitive information, it is crucial to establish a data classification system that categorizes data based on its sensitivity and criticality. In this task, you will define three data types (confidential, internal, and public) and classify the datasets provided by the data warehouse team accordingly.

- Define each of the three data types: confidential, internal, and public
- Categorize each dataset provided by the data warehouse team into one of the three data types

Data Classification

Confidential: It includes information that, if leaked to unauthorized individuals, will have a catastrophic effect on the organization, its employees, and its end users.
Internal: It contains information that is not intended for public disclosure and is not as sensitive as confidential data, but this information is used internally among organization departments, employees, and business partners. This information contains company policies, internal reports, etc. that, if leaked to the public, will have a significant impact on the organization.
Public: The data is intended to be freely shared with the public. This data poses no risk to an organization. Anyone can access public data. Public data contains blog posts, marketing materials, and any intentionally publicly available information by an organization.

Categorize each dataset into one of the three data types

Dataset	Data Type
Employee profile data	Confidential
Customer profile data	Confidential
Company email	Internal
Repository of previously published blogs	Public
Internal employee newsletters	Internal
Technology engineering diagrams	Confidential
Intellectual property	Confidential

Data Regulations

It is essential to understand the regulatory landscape surrounding the company's data assets. Different data types may be subject to various regulations, depending on their sensitivity and the nature of the information they contain. In this task, you will identify the regulations that apply to each data type (confidential, internal, and public) and provide a justification for why each regulation applies.

- For each data type (confidential, internal, and public), identify the relevant data regulations (if any)
- Provide a justification for why each identified regulation applies to the specific data type

Data Regulations

Confidential	GDPR: Any personally identifiable information (PII), including name, address, father's name, financial information, and biometric data, as well as sensitive personal data, such as health records, is subject to the GDPR. HIPPA: HIPPA applies to protected health information (PHI). If PHI includes protected health information, then HIPPA regulations apply. HIPAA enforces strict controls on how to store, access, and transmit confidential PHI. PCI DSS: For those organizations that handle credit card information, PCI DSS compliance is mandatory. confidential data containing cardholder information must be protected by the applicable organizations.
Internal	Sarbanes-Oxley Act (SOX): SOX requires that internal data, particularly financial data should be securely maintained. Federal Information Security Management Act (FISMA):FISMA requires that the internal data involving government contractors should be protected according to standards. Gramm-Leach-Bliley Act (GLBA):Financial institutions are subject to the Gramm-Leach-Bliley Act (GLBA), which focuses on internal customer data that contains non-public personal information (NPI) that needs to be protected. This regulation's primary objective is to safeguard the integrity and confidentiality of internal data.
Public	Freedom of Information Act (FOIA): It applies to government agencies. None (for purely public data): Public data generally does not fall under specific regulatory requirements because this information is intentionally available to the public. However, public data should be accurate and should not expose any sensitive information. Fair Use Doctrine (for copyrighted content) If any data is subject to copyright laws, then it must adhere to the fair use doctrine. That allows limited use of copyrighted material without requiring permission from the right holder if certain conditions are met.

Regulatory Compliance

Your responsibilities include recommending and implementing security controls that ensure compliance with applicable data regulations. By establishing clear security policies and procedures, you can help the company meet its regulatory obligations and protect sensitive data from unauthorized access, use, or disclosure. In this task, you will design six security policy items that address the requirements of the identified regulations relevant to JFin Payments' data.

- Write six security policy items that address the requirements of the applicable data regulations
- Each policy item should be written in clear, concise language and follow the provided format
- The policy items should cover various aspects of data security, such as data encryption, access control, data disposal, and breach notification

Regulatory Compliance

Data Encryption Policy:

All types of confidential or sensitive data either at rest or in transit, must be encrypted using any strong encryption algorithm such as AES-256.

This policy ensures compliance with PCI DSS, CCPA, and GDPR.

Access Control Policy:

Only authorized individuals should be able to access confidential data in any way. It is recommended to create role-based access control (RBAC) and to regularly store, monitor, and review all forms of access logs.

The GDPR's data minimization principle is adhered to by this policy

Data Disposal and Retention Policy:

The data that is classified as confidential should be securely disposed of after the retention period has expired. Disposal methods must contain data wiping or physical destruction of storage media.

HIPPA and GDPR require secure disposal of personal data to prevent unauthorized access.

Breach Notification Policy:
In a scenario of a data breach, all the affected individuals such as users, employees, any business partners, and relevant regulatory bodies should be notified within 27 hours.
GDPR Article 33 requires the breach notification should include the nature of the breach, the types of data involved, and the steps taken to mitigate it.

Data Classification and Handling Policy:
Based on the confidentiality, sensitivity, and regulatory requirements, all data of an organization should be classified as confidential, internal, or public. All the data handling processes and procedures such as storage, transmission, and sharing must follow classification to ensure compliance with GDPR, PCI DSS, and other relevant regulations.

Third-Party Vendor Management Policy:
All third-party vendors that process or store JFin Payments' data must adhere to the same security standards as JFin Payments. Conducting regular security assessments and ensuring that vendors comply with applicable data protection regulations such as GDPR and CCPA.

Section Two:
Data Confidentiality

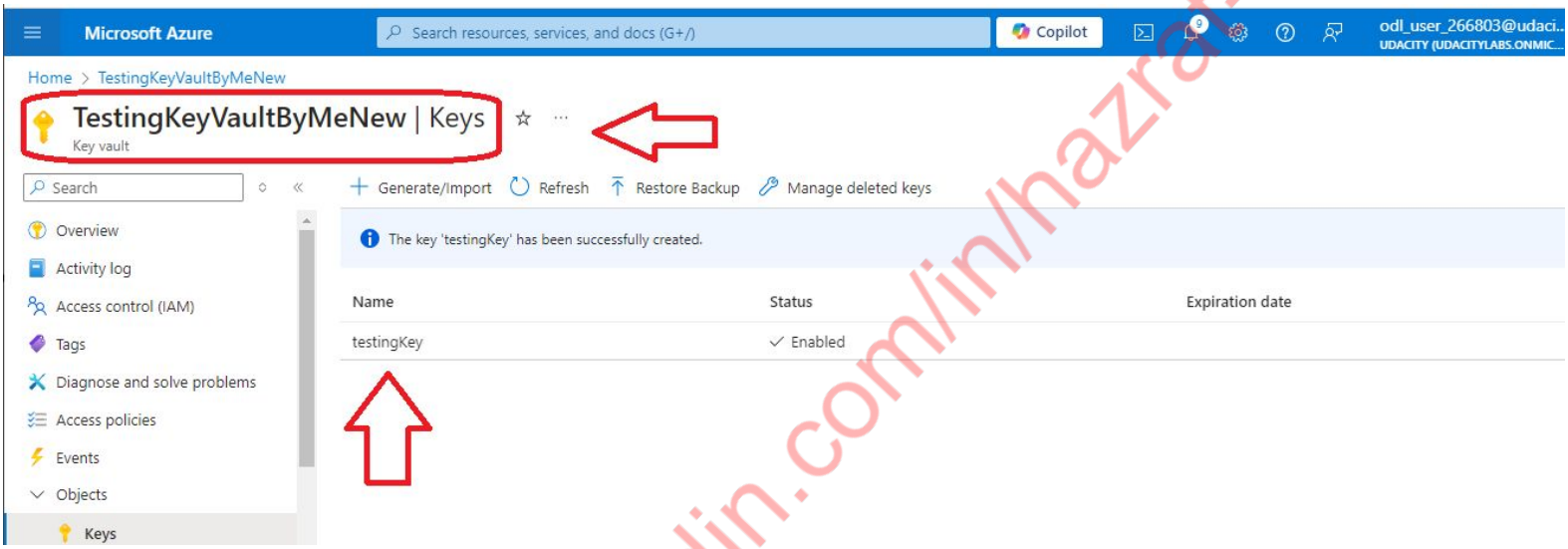
Securing Disks

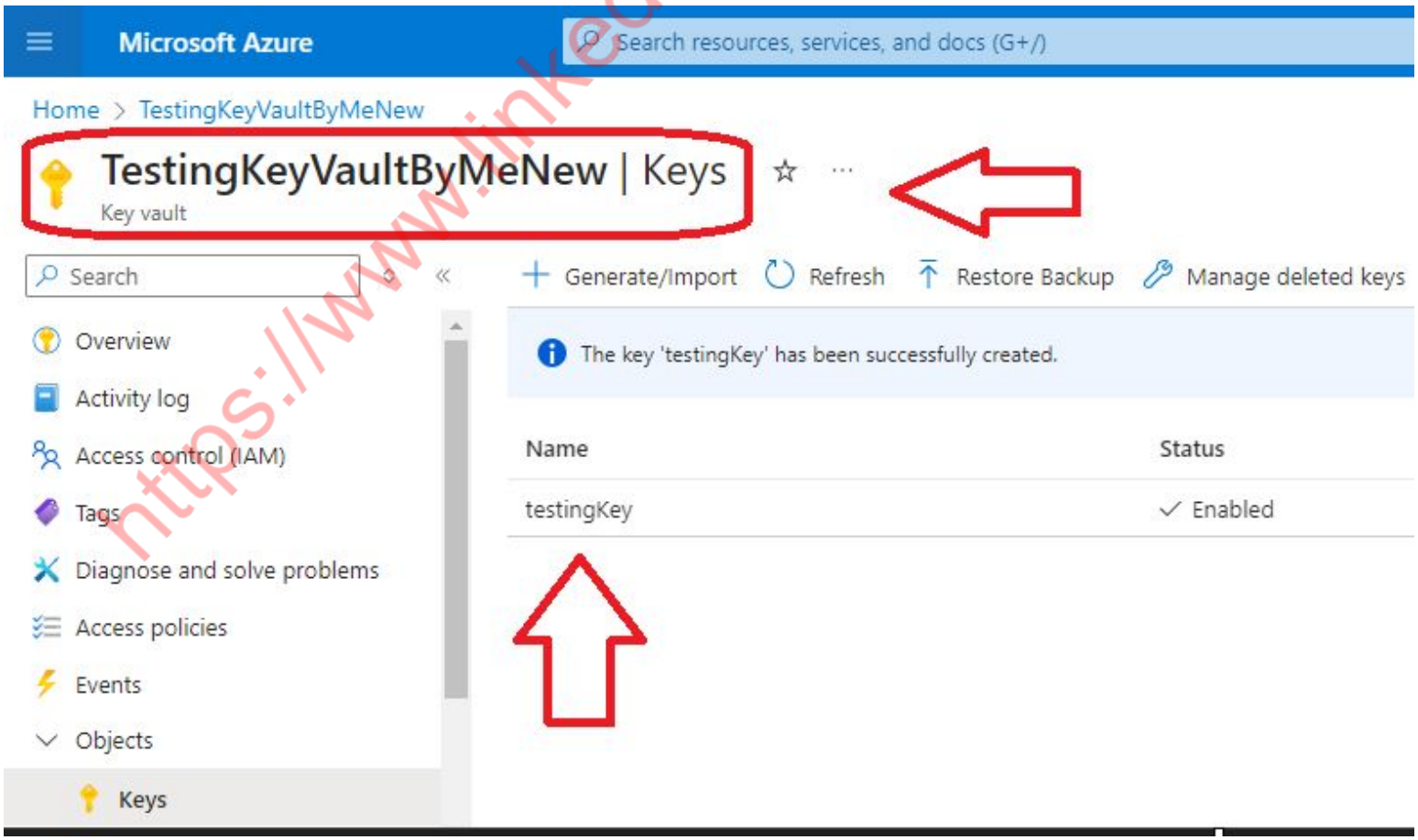
As a Data Security Analyst at JFin Payments, one of your responsibilities is to ensure the confidentiality and integrity of data stored on virtual disks. Implementing disk encryption using strong cryptographic keys is an effective way to protect sensitive data from unauthorized access. In this task, you will generate an RSA key (2048 bits) and leverage it to enable encryption on a disk, providing evidence of successful implementation through screenshots.

- Generate an RSA key (2048 bits) for disk encryption
- Create a disk encryption set using the generated RSA key
- Create a disk and encrypt it with the disk encryption set
- Provide the following screenshots as evidence of successful implementation:
  - Screenshot 1: Successful key generation page
  - Screenshot 2: Successful creation of disk encryption set page
  - Screenshot 3: Successful disk encryption page

Securing Disks

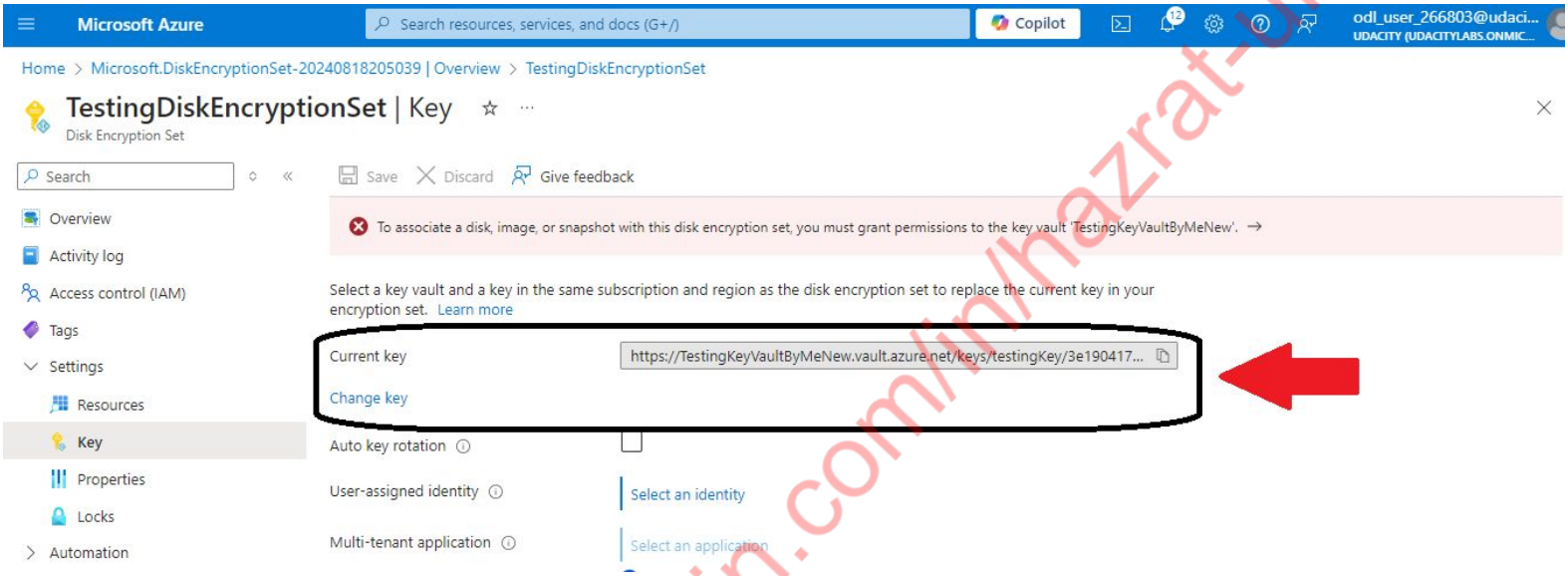
Place the screenshot from the Keys page of the Key Vault you created, with the generated key.

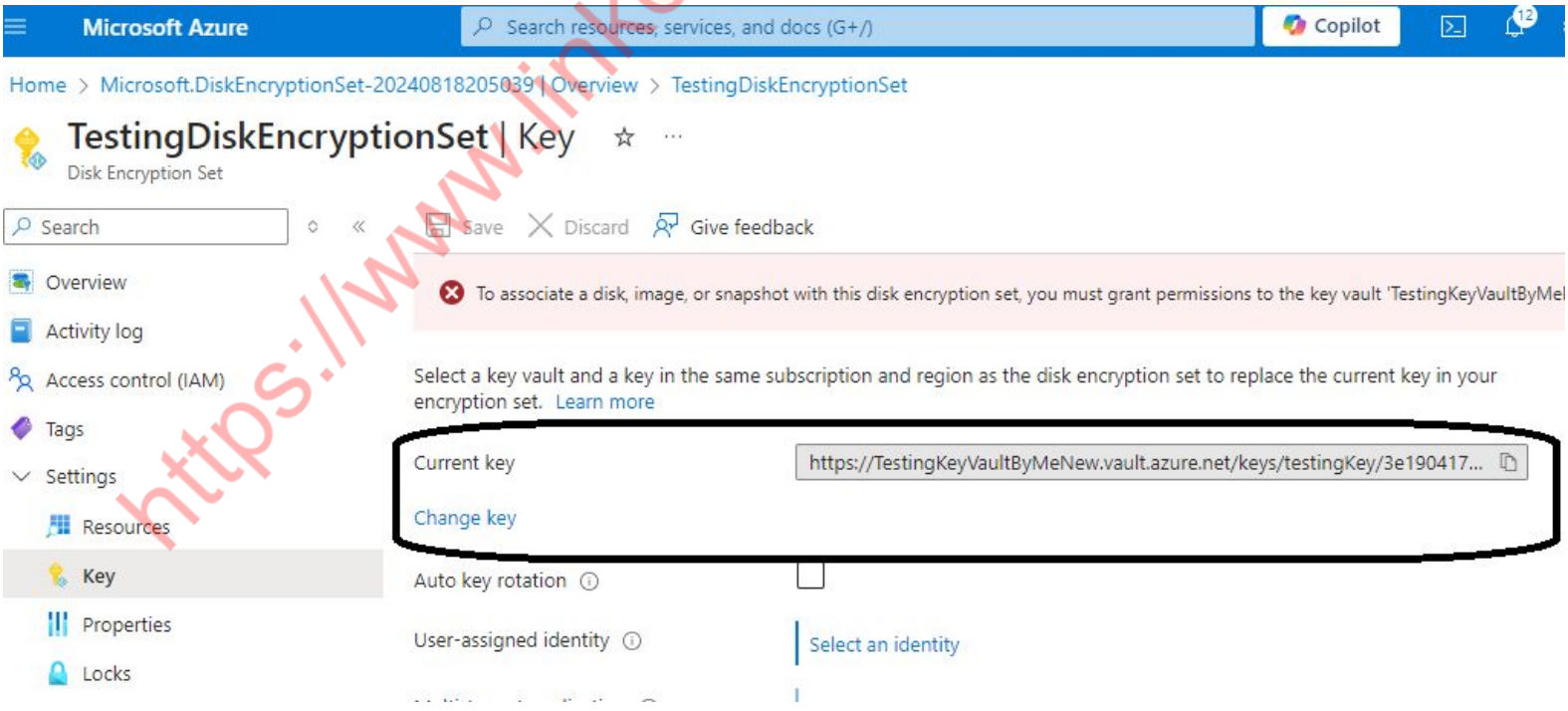




Securing Disks

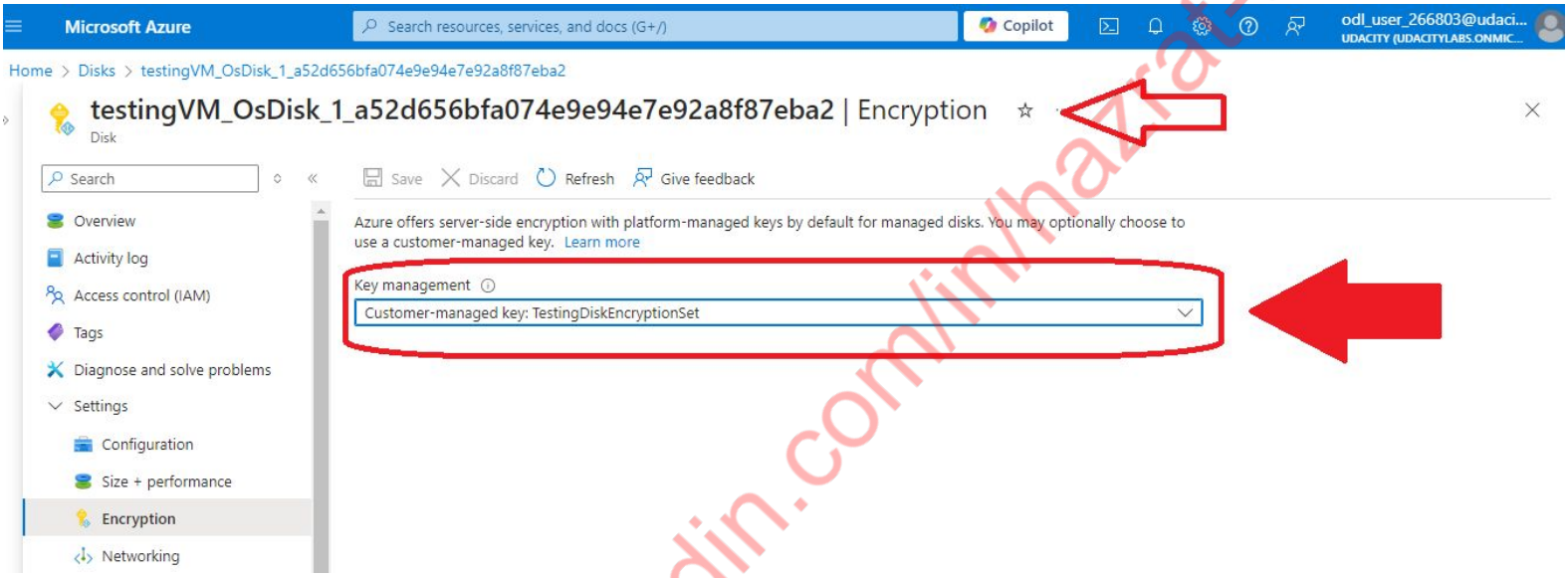
Place the screenshot from Key page of the Disk Encryption Set you created

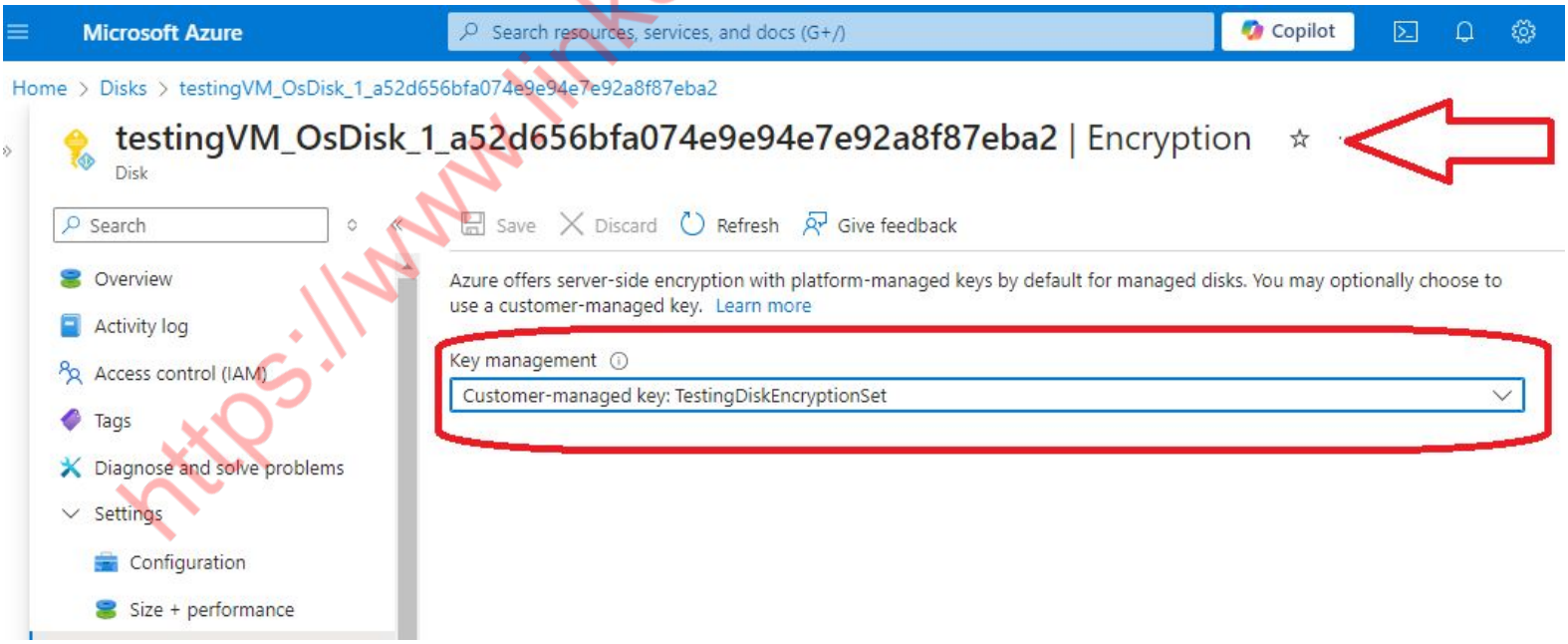




Securing Disks

Place the screenshot from the Encryption page of the Disk you created





Section Three: Data Integrity

File Integrity Verification

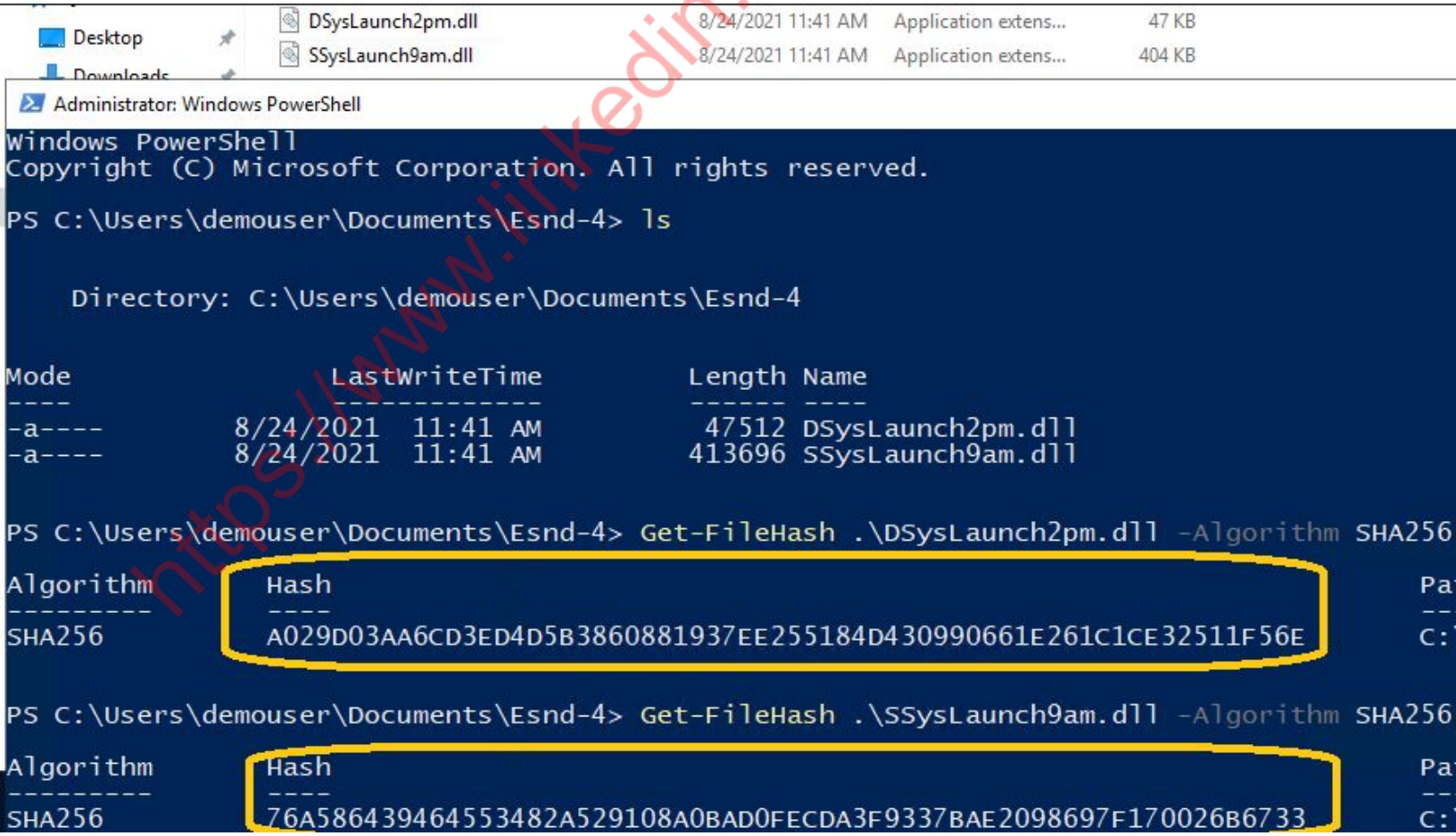
ensuring the integrity of critical files is essential to maintain the security and reliability of the company's systems. One common method for verifying file integrity is by generating and comparing cryptographic hashes, such as SHA256. In this task, you will generate SHA256 hashes for two files in the "Documents/Esnd-4/" folder and compare them with the provided hashes on the next slide. By analyzing the results, you will determine whether the files have maintained their integrity or if they have been tampered with. Additionally, you will submit a screenshot of the generated hashes as part of your evidence.

- Locate the two files in the "Documents/Esnd-4/" folder on the VM
- Generate SHA256 hashes for each of the two files
- Compare the generated hashes with the original hashes on the next slide and explain what your findings mean in terms of file integrity
- Submit a screenshot of the generated hashes

File Integrity Verification

The original DSysLaunch2pm.dll hash: B029D03AA6CD3ED4D5B3860881937EE255184D430990661E261C1CE3251184D4
The original SSysLaunch9am.dll hash: 76A586439464553482A529108A0BAD0FECDA3F9337BAE2098697F170026B6733

Only DSysLaunch2pm.dll is changed while the SSysLaunch9am.dll file remained unchanged. It means that there is some changes made to DSysLaunch2pm.dll because the original file hash does not match to the generated file hash. But SSysLaunch9am.dll file original hash matches with the generated hash to this file is not changed.



File Integrity Verification

Generated Hashes:

```
PS C:\Users\demouser\Documents\Esnd-4> Get-FileHash .\DSysLaunch2pm.dll -Algorithm SHA256

Algorithm       Hash                                                                   Pat
---------       ----                                                                   ---
SHA256          A029D03AA6CD3ED4D5B3860881937EE255184D430990661E261C1CE32511F56E       C:\

PS C:\Users\demouser\Documents\Esnd-4> Get-FileHash .\SSysLaunch9am.dll -Algorithm SHA256

Algorithm       Hash                                                                   Pat
---------       ----                                                                   ---
SHA256          76A586439464553482A529108A0BAD0FECDA3F9337BAE2098697F170026B6733       C:\
```

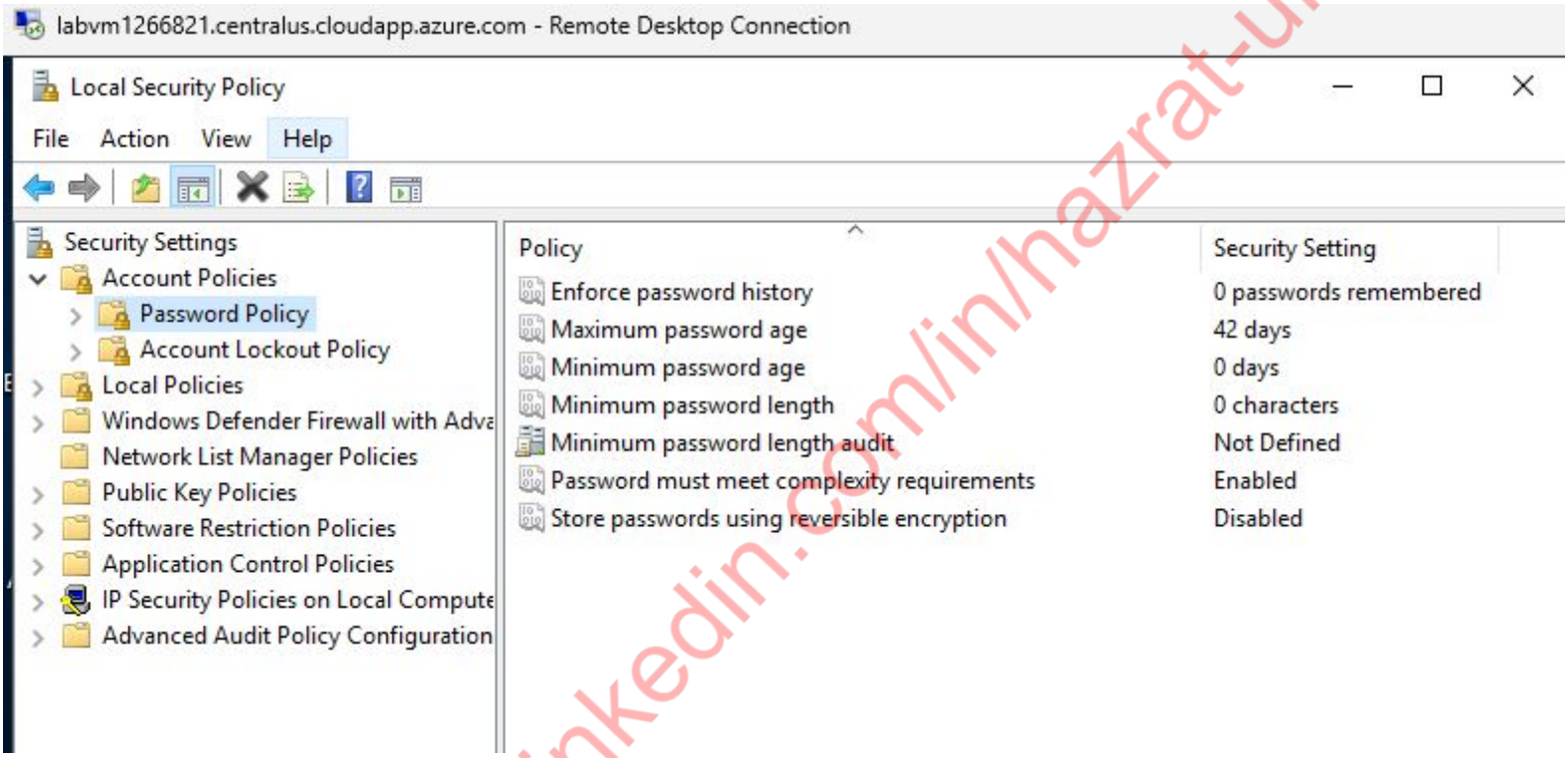
Auditing Security Settings

It is crucial to ensure that the company's virtual machines (VMs) are properly configured to maintain the security and integrity of the systems and data they host. Auditing the security settings of VMs helps identify potential vulnerabilities and ensures compliance with industry best practices and regulatory requirements. In this task, you will access the audit settings on a VM and provide screenshots as evidence of the password policy, account lockout policy, audit policy, and security options configurations.

- Navigate to the password policy screen and take a screenshot
- Navigate to the account lockout policy screen and take a screenshot
- Navigate to the audit policy screen and take a screenshot
- Navigate to the security options screen and take a screenshot
- Ensure that all screenshots are clear, legible, and capture the relevant information

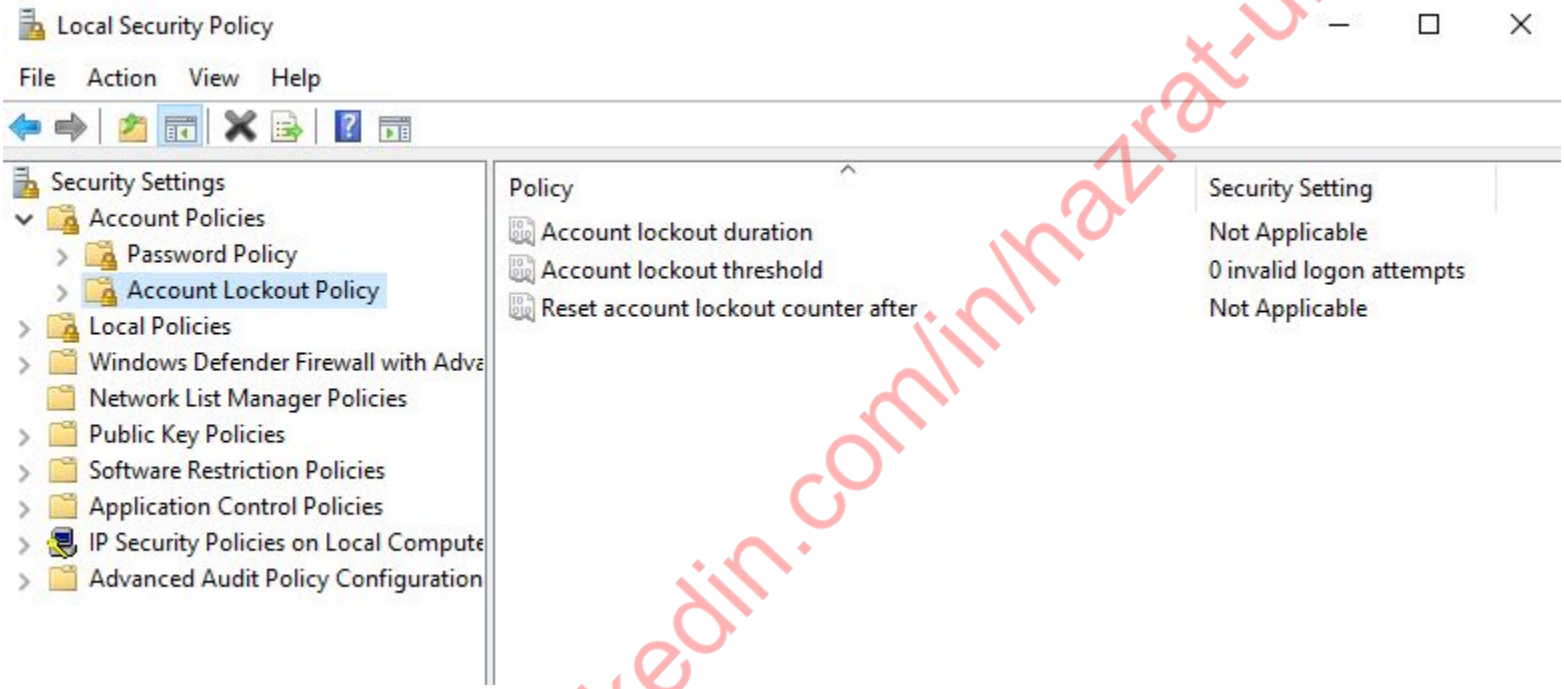
Auditing Security Settings

Place the screenshot of the password policy screen here



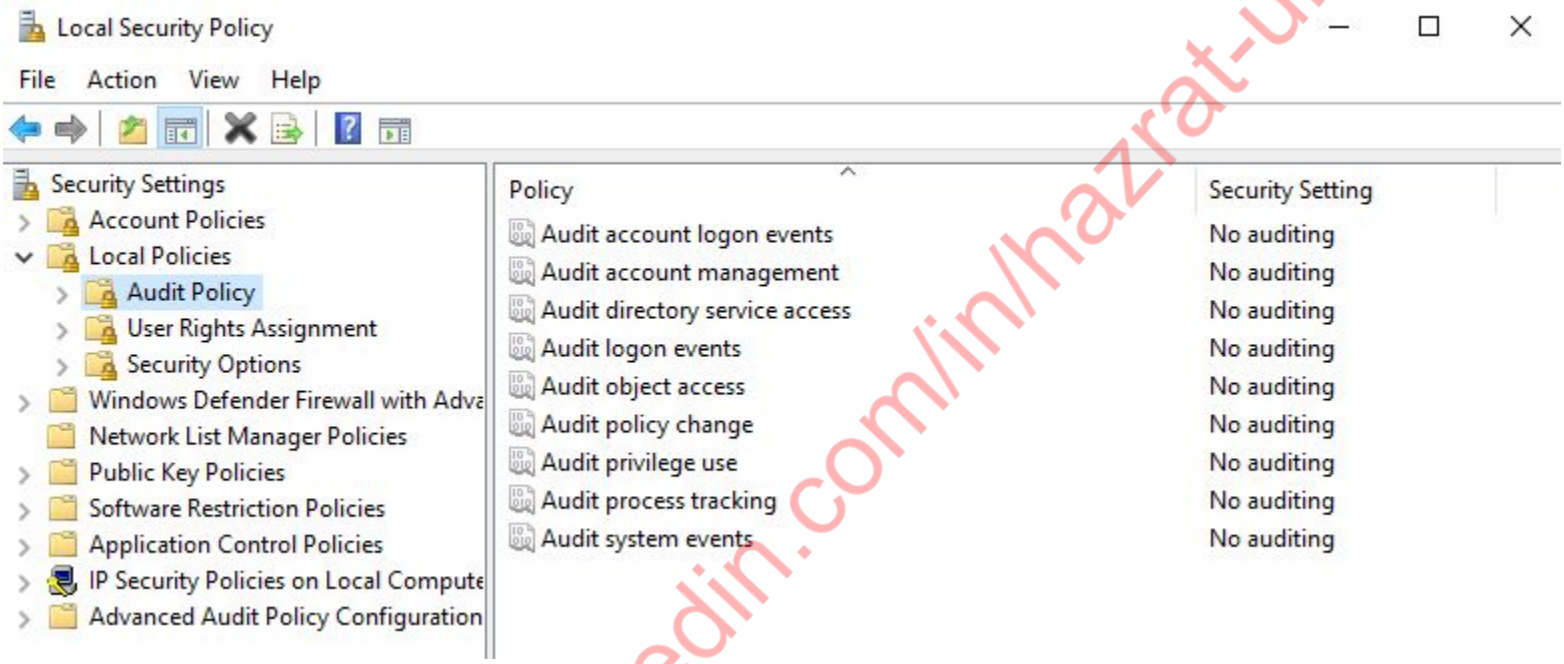
Auditing Security Settings

Place the screenshot of account lockout policy screen here



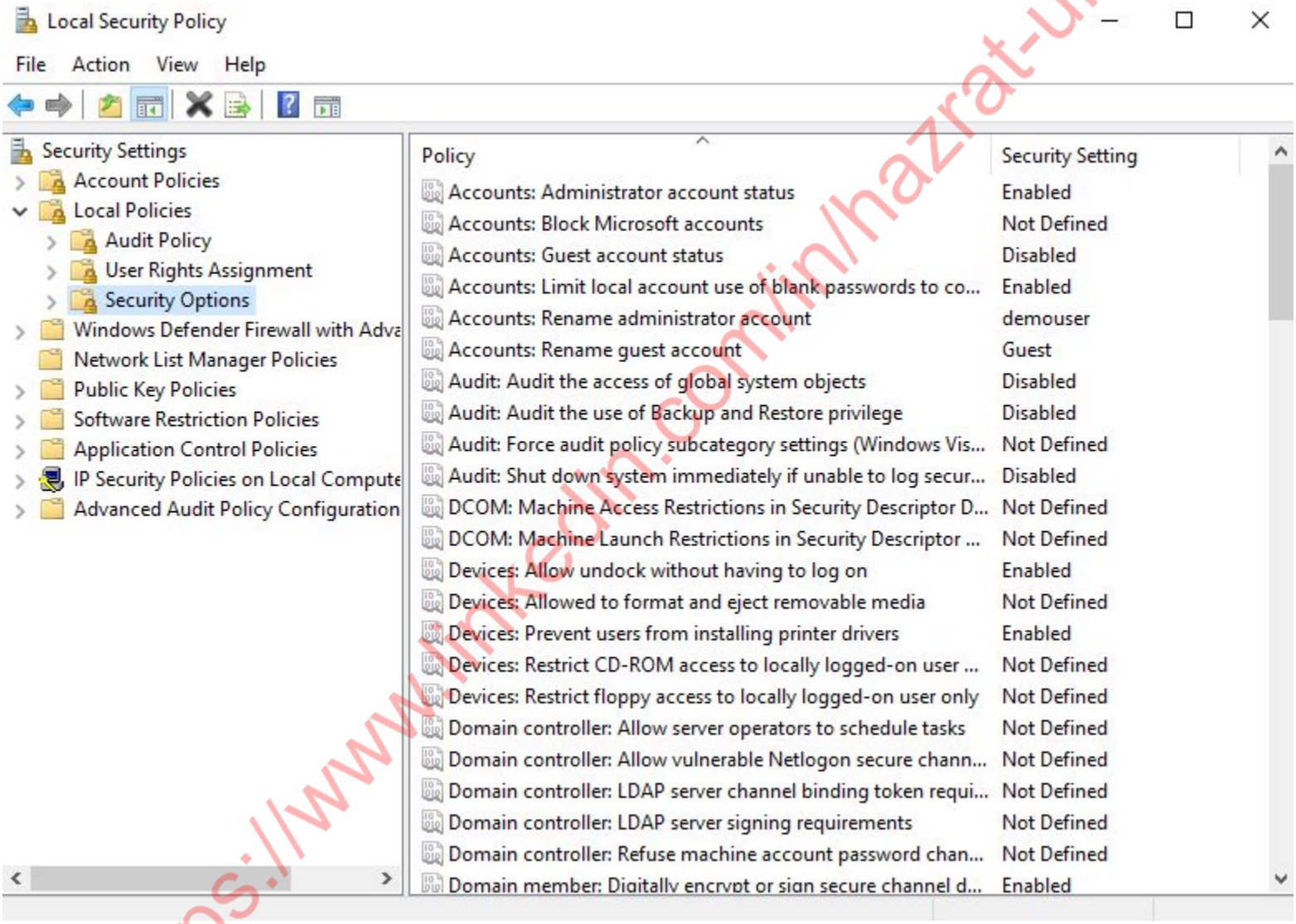
Auditing Security Settings

Place the screenshot of the audit policy screen here



Auditing Security Settings

Place the screenshot of the security options screen here



Enhancing VM Security

The next step is to provide actionable recommendations based on your findings. Review the existing security policies and options on the VM and provide 4 specific security recommendations that the company should implement on the machine to strengthen its overall security posture and comply with industry best practices and regulatory requirements. You do not need to implement any of this.

- Review the password policy, account lockout policy, audit policy, and security options of the VM
- Identify areas where security improvements can be made based on industry best practices and security standards
- Provide 4 specific security recommendations that the company should set on the machine
- For each recommendation, include a brief justification explaining the benefits and importance of the proposed setting

Enhancing VM Security

1. Enforce a password history policy.

This policy prevents users from entering old passwords again. It helps ensure that passwords are regularly changed to maintain security and comply with industry best practices.

2. Implement an account lockout policy.

This policy helps in preventing brute force attacks by locking out those accounts on which several failed login attempts are made. It also reduces the risk of denial-of-service (DOS) attacks if we set the appropriate lockout duration and reset time.

3. Enable comprehensive auditing.

enable auditing for critical events such as:

Audit account logon events
audit account management
Audit logon events
audit system events
Audit policy change

By enabling these audit logs, you can easily track and monitor potentially malicious activities and any type of unauthorized access. This also helps us in incident repose and forensic analysis and ensures compliance with regulatory requirements such as GDPR, HIPPA, and PCI DSS.

4. Restrict the use of Microsoft accounts.

Allowing the use of Microsoft accounts in enterprises can introduce security risks. By blocking your Microsoft account, you can ensure that only domain accounts are used that are managed by your organization.

Section Four: Data Availability

Developing a Data Backup Strategy

In the previous task, you categorized JFin Payments' data into confidential, internal, and public data types and identified the applicable regulations for each category. Building upon this foundation, it is essential to establish a robust data backup strategy to ensure data availability, integrity, and compliance with regulatory requirements. In this task, you will recommend a backup frequency and retention period for each data type, providing justifications for your recommendations based on industry best practices and regulatory obligations. Although multiple different backups are needed for each data type, **only recommend the shortest amount of time appropriate between backups for the data type**.

- Recommend a backup frequency for each data type, specifying at least how often a backup should be run (e.g., real-time, daily, weekly, as needed)
- Propose a retention period for each data type, indicating how long the backups should be kept (e.g., 30 days, 90 days, 1 year)
- Provide justifications for your recommended backup frequency, considering factors such as data criticality, regulatory requirements, and industry best practices

Developing a Data Backup Strategy

Confidential Data	
Backup Frequency:	Real time
Retention Period:	180 days

Justification:

Confidential data is highly sensitive and critical to JFin's Payments operations. This category contains personally identifiable information (PII), payment card information (PCI), and different types of financial records, all of which are subject to GDPR, PCI, DSS, and CCPA.

Real-time backups help in ensuring that if there is any change or addition to the data, that data is immediately backed up. It reduces the risk of data loss due to different cyber attacks and system failures. The 180-day retention period aligns with industry best practices and compliance regulations

Internal Data	
Backup Frequency:	Daily
Retention Period:	90 Days

Justification:

Internal data is not as sensitive as confidential data, but it is still mandatory for business operations. This category of data may contain different types of internal communications, letters to employees, internal project documentation, etc.

Performing daily backups will help capture any changes that occur within 24 hours of operation. The 90-day retention period is recommended based on industry standards.

Developing a Data Backup Strategy

Public Data	
Backup Frequency:	Weekly
Retention Period:	45 Days
Public data is data that is least sensitive and is intentionally shared with the public. Public data contains public-facing web pages, different types of reports for the public, marketing materials, etc. Due to its less sensitive nature, public data needs to be backed up weekly, and there should be a 45-day retention period for public data, according to industry best practices.	

Creating a Backup

Continuing our focus on data protection and disaster recovery, creating regular backups of critical systems is essential to ensure data availability and minimize downtime in case of incidents or failures. In this task, you will create a backup of the LabVM and provide a screenshot of the LabVM Backup screen as proof of initiation.

- Start the backup process for the VM in Azure
- Take a screenshot of the VM Backup screen, clearly showing the initiated backup process
- You do not need to wait until the backup process is finished

Creating a Backup

Place the screenshot of the LabVM Backup screen here