Data Security Analysis

Project Scenario

Overview

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 1: 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.
[Performing annual data classification ensure that information assets are consistently identified and manage according to their sensitivity and business importence. Benefits : ● Strengthens data security by ensuring sensitive information receives the highest level of protection. ● Supports regulatory compliance through clear categorization aligned with privacy laws and standards. ● Improves risk management by identifying which data sets require enhanced controls and monitoring, and also making it easier to identify and mitigate exposure of critical data. ● Improves operational efficiency by streamlining access controls and prioritizing resource allocation based on data sensitivity, and also will help reducing duplication, mismanagement and unnecessary data storage.]
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 prioritize protection efforts for the organization's most vital assets, protective measures for key operational and financial systems. Benefits: ● Protects Business continuity through proactive identification of mission-critical systems needing stronger resilience and monitoring. ● Promotes proactive risk management by detecting dependencies and vulnerabilities early. ● Ensure cyber security controls are applied effectively to high-impact systems, improving overall defence posture. ● Promotes efficient resource allocation by focusing maintenance, updates and security investments where they matter most.]
IT Staff should perform a regulatory assessment annually, or when there are notable business or technology changes.
[Conducting annual regulatory assessments allows the organization to stay current with changing compliance obligations and industry standards. Benefites: ● Maintains regulatory compliance, avoiding penalties and reputational damage. ● Enables early detection of compliance gape and implementing corrective actions promptly. ● Strengthens governance and accountability by aligning company policies with external regulations and standards. ● Enhances stakeholder confidence through demonstrable commitment to lawful and ethical data management practices.]

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: [Confidential data refers to information that requires strict access controls, and is protected by laws, regulations, or organizational policies. Unauthorized access or disclosure can lead to significant harm, such as legal penalties, financial loss or reputational damage. Examples : Social security numbers, credit card details, medical records and employee personal information.]
Internal: [Internal data is information that is only accessable to employees and authorised personnel within an organization. It is not intended for public release and is used for internal operations, decisionmacking or business planning. Examples : internal memos, business strategies, financial reports, system IP addresses.]
Public: [Public information is information that is freely accessable to anyone, both inside and outside the organization. It poses minimum risk if disclosed and is often used for transparency or marketing purposes. Examples : press releases, company names, job descriptions.]

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 (General Data Protection Regulation), PCI DSS (Payment Card Industry Data Security Standard), HIPAA (Health Insurance Portability and Accountability Act), DPDP Act (Digital Personal Data Protection Act, 2023)]: [Justification : Confidencial data includes personal information, helth data, payment card information or other sensitive business data. GDPR applies to protect personal data of EU residents, Mandating strict controls, Consent requirements, accurate maintenance, breach notification within 72 hours and related protections. PCI DSS regulates payment card data security. HIPAA Covers sensitive helth information requring confidentiality. Indiai's DPDP Act protects digital personal data by requiring transparency consent, purpose limitation, and security measures. These laws apply to confidential data due to it's sensitivity involving individual privacy and financial details,requiring rigorous protection to prevent privacy breaches, identity theft and financial fraud.]
Internal	[GDPR (General Data Protection Regulation), DPDP Act (Digital Personal Data Protection Act, 2023)]: [Justification : Internal data typically involves company operational data, employee data and sometimes financial information not openly shared publicly but critical for internal process. GDPR and DPDP apply if the internal data contains personal information requiring lawful processing and protection. these regulation address internal data to preserve business integrity, compliance, employee privacy, and prevent insider threats.]
Public	[Regulatory focus is lighter, but have certain limitations.]: [Justification : Public data is generally non-sensitive information intended for wide dissemination or public access. However, if public data contains personal information accidentally disclosed, GDPR or similar privacy laws still apply.]

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 sensitive payment card data and personal customer information must be encrypted both in transit and at rest using strong encryption standards such as AES-256 to prevent unauthorized access.]
[**Access Control Policy**: Access to sensitive data systems will be granted on a strict need-to-know basis through role-based access controls (RBAC). Multi-factor authentication (MFA) is mandatory for all users accessing payment or personal data environments.]
[**Data Disposal Policy**: All sensitive data that is no longer required for business or regulatory purposes must be securely disposed of immediately through methods such as secure deletion or physical destruction, ensuring data cannot be recovered.]
[**Security Incident and Breach Notification Policy**: In the event of a data breach or suspected security incident affecting customer or payment data, an incident response process must be immediately initiated with notification to regulatory authorities and impacted individuals as required by applicable laws.]
[**Network Security Policy**: Firewall and intrusion detection/prevention systems must be implemented and continuously monitored to protect the payment data environment from unauthorized external and internal network threats.]
[**Employee Training and Awareness Policy**: All employees must receive regular training on data protection regulations, secure data handling procedures, and security incident reporting to maintain awareness and reduce human error risks.]

Section 2: Data Confidentiality

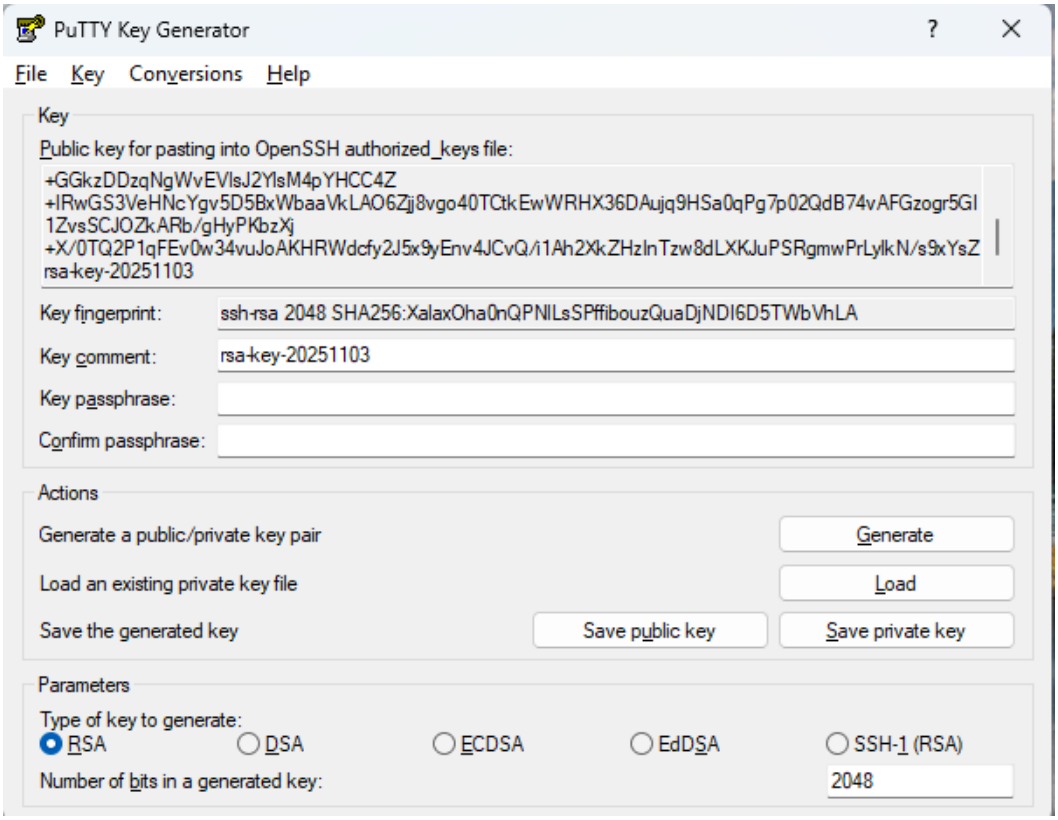
Securing Disks

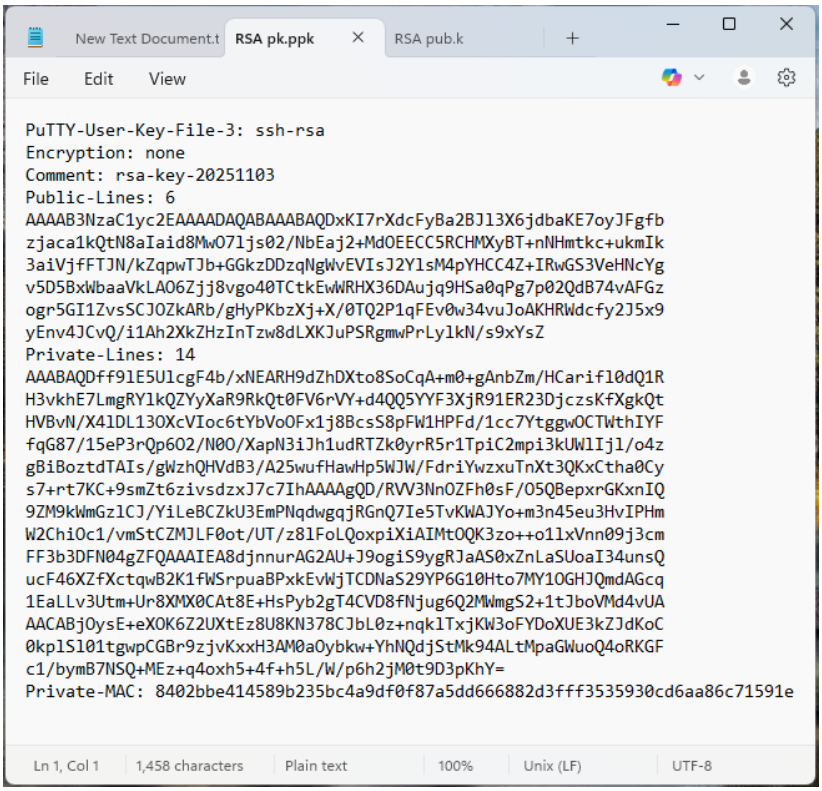
As a Data Security Analyst at JFin Payments, one of your responsibilities is to ensure the confidentiality and integrity of data stored on virtual disks. Implementing disk encryption using strong cryptographic keys is an effective way to protect sensitive data from unauthorized access. In this task, 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

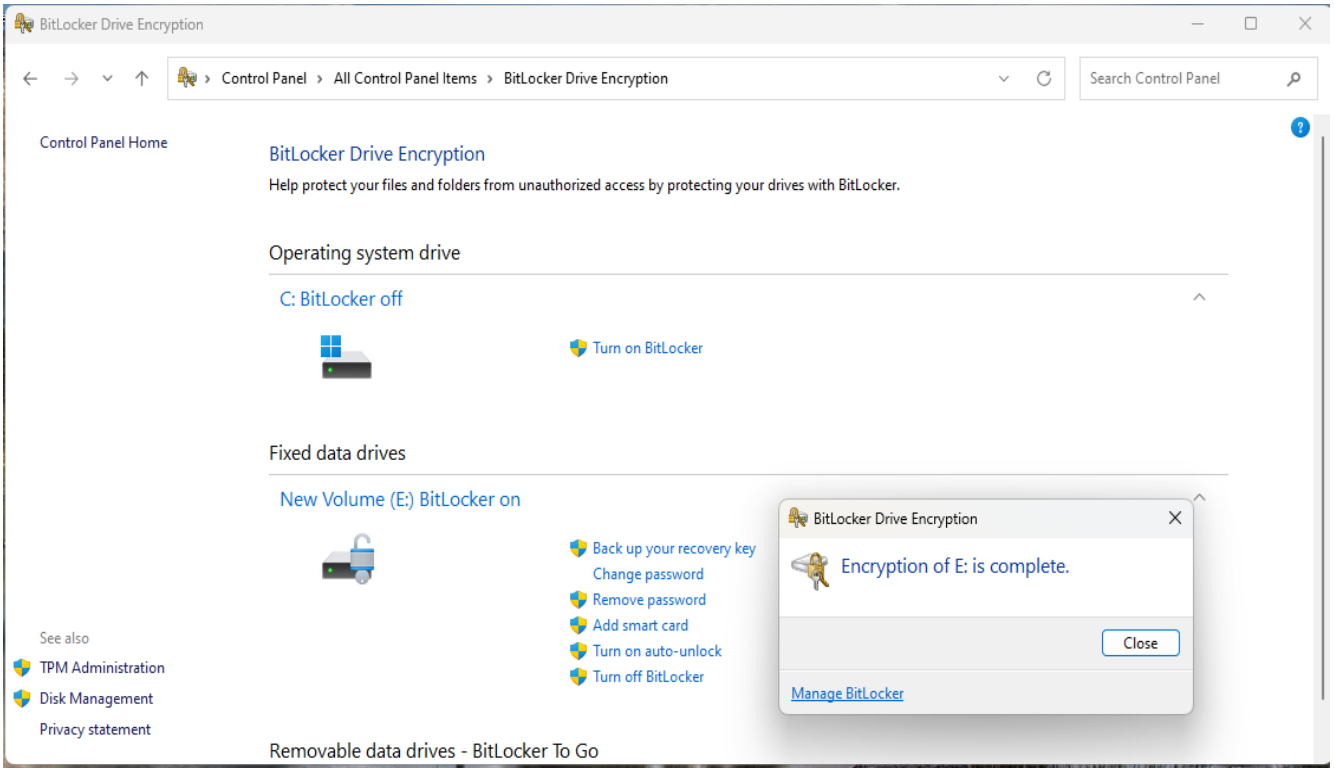
Place the screenshot of the generated key.

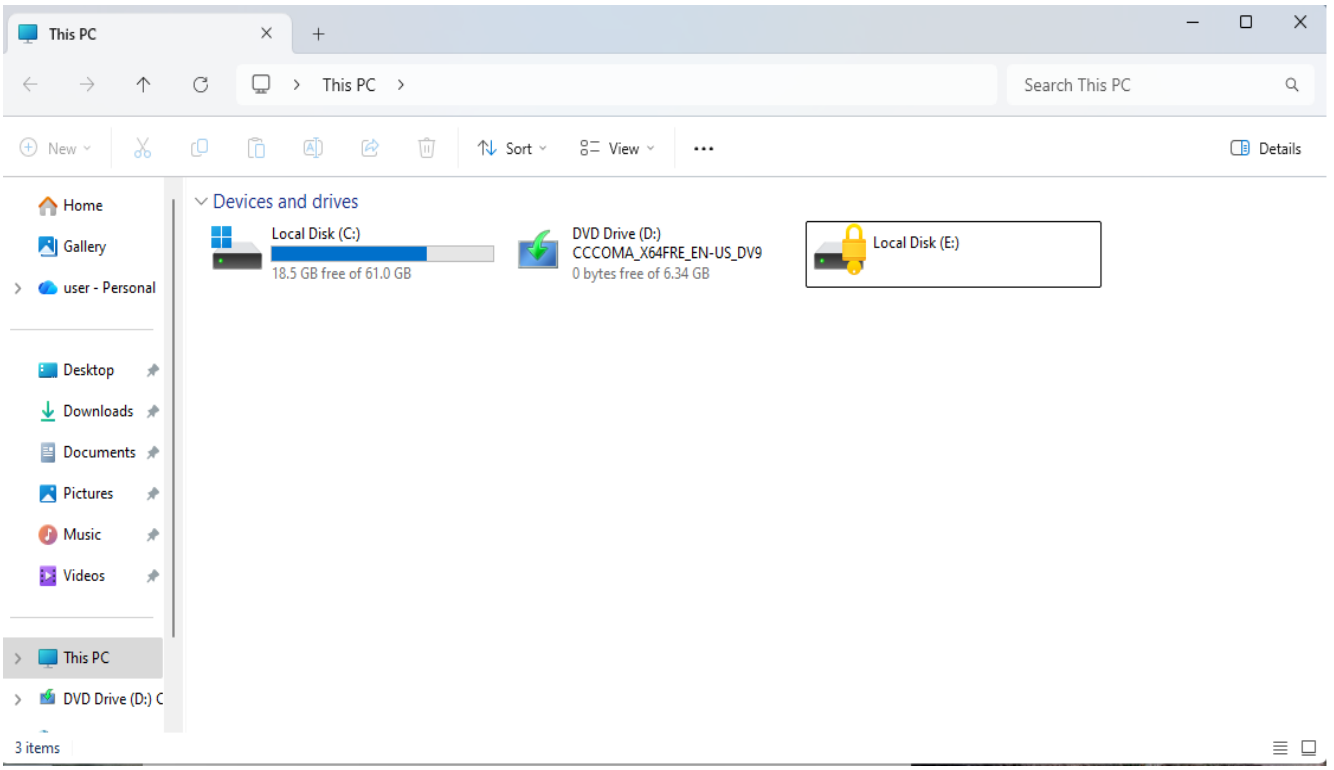




Securing Disks

Place the screenshot from configuration Page after you have encrypted the Virtual Disk Image of the VM





Section 3: 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 public files Additionally, you will submit a screenshot of the generated hashes as part of your evidence.

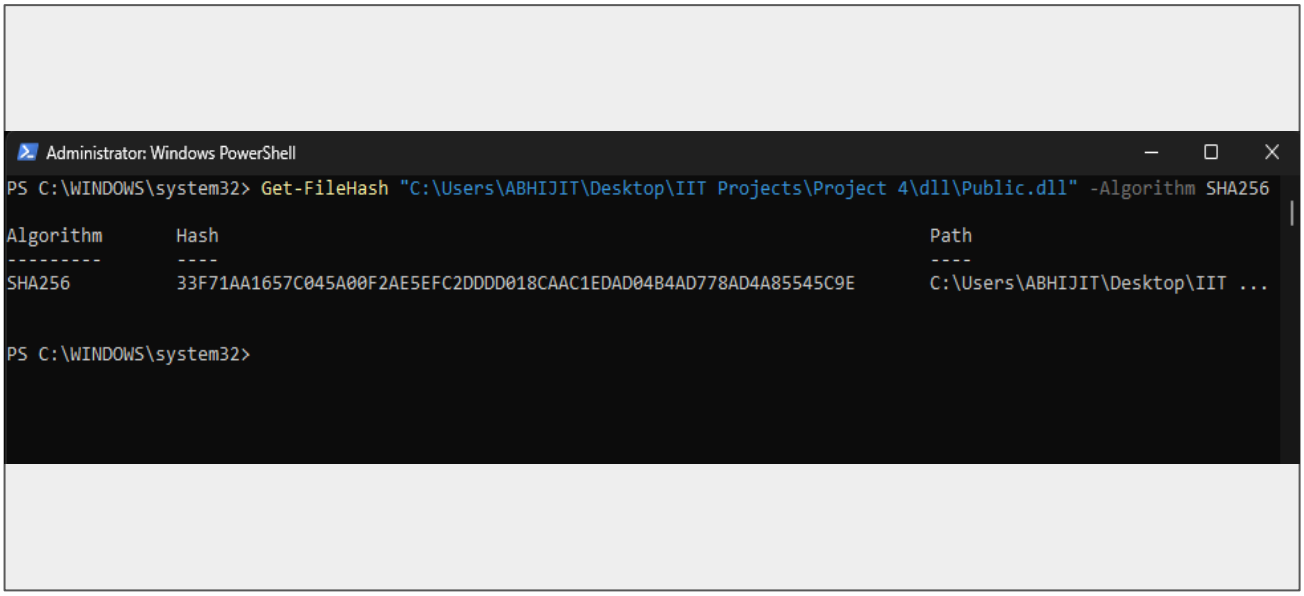
- Go to https://drive.google.com/file/d/1XT0Uc1Q4FWtRAxhfX1m9DsXhU599ytv0/view?usp=drive_link
- Generate SHA256 hashes
- Compare the generated hashes with the original hashes on the next slide and explain what your findings mean in terms of file integrity
- Submit a screenshot of the generated hashes

File Integrity Verification

Download public.dll from dll-files.com and verify Hash.

Version 14.0.0.130
The original public.dll hash: f7761cd21b7461fd126ecbac1fa7e516138349fb

[The files have been modified. The hash valu is not same.]



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

Steps to get Local Security Policy

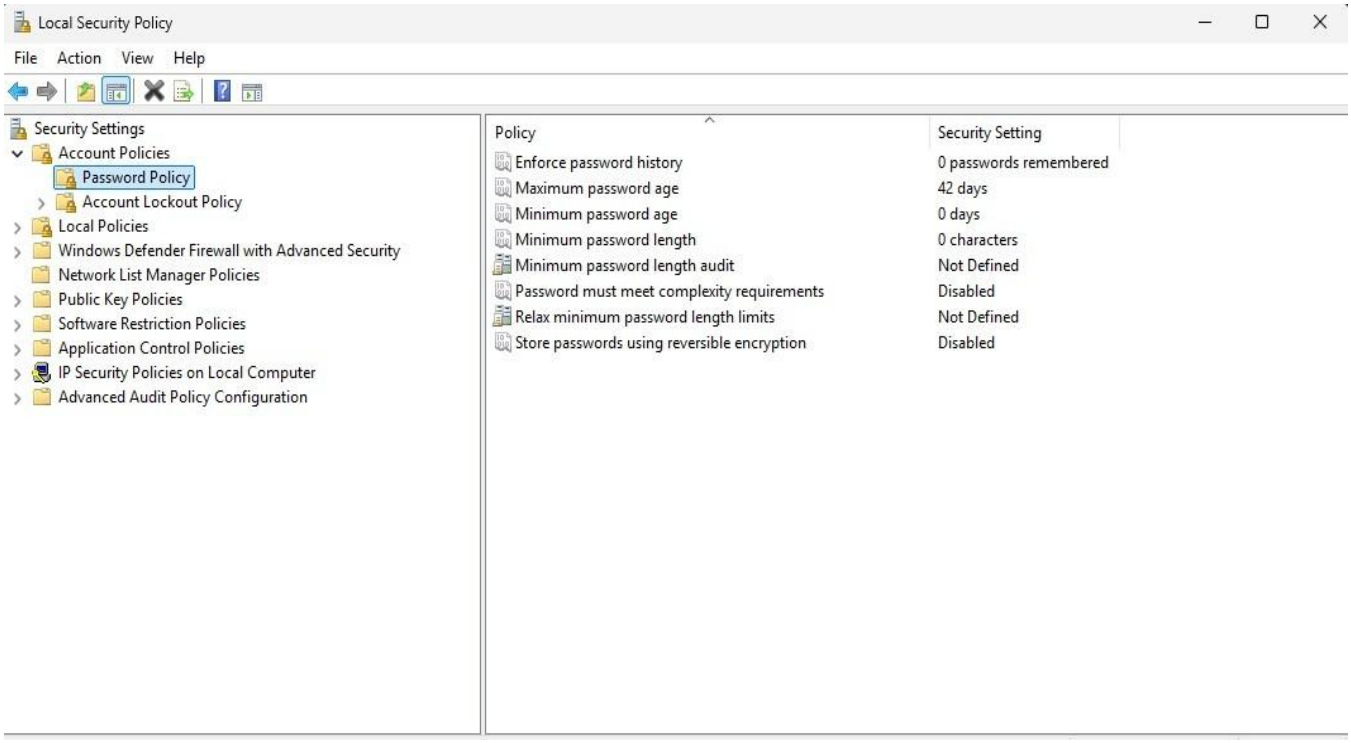
```
@echo off
pushd "%~dp0"

dir /b %SystemRoot%\servicing\Packages\Microsoft-Windows-GroupPolicy-ClientExtensions-Package~3*.mum >List.txt
dir /b %SystemRoot%\servicing\Packages\Microsoft-Windows-GroupPolicy-ClientTools-Package~3*.mum >>List.txt

for /f %%i in ('findstr /i . List.txt 2^>nul') do dism /online /norestart /add-package:"%SystemRoot%\servicing\Packages\%%i"
pause
```

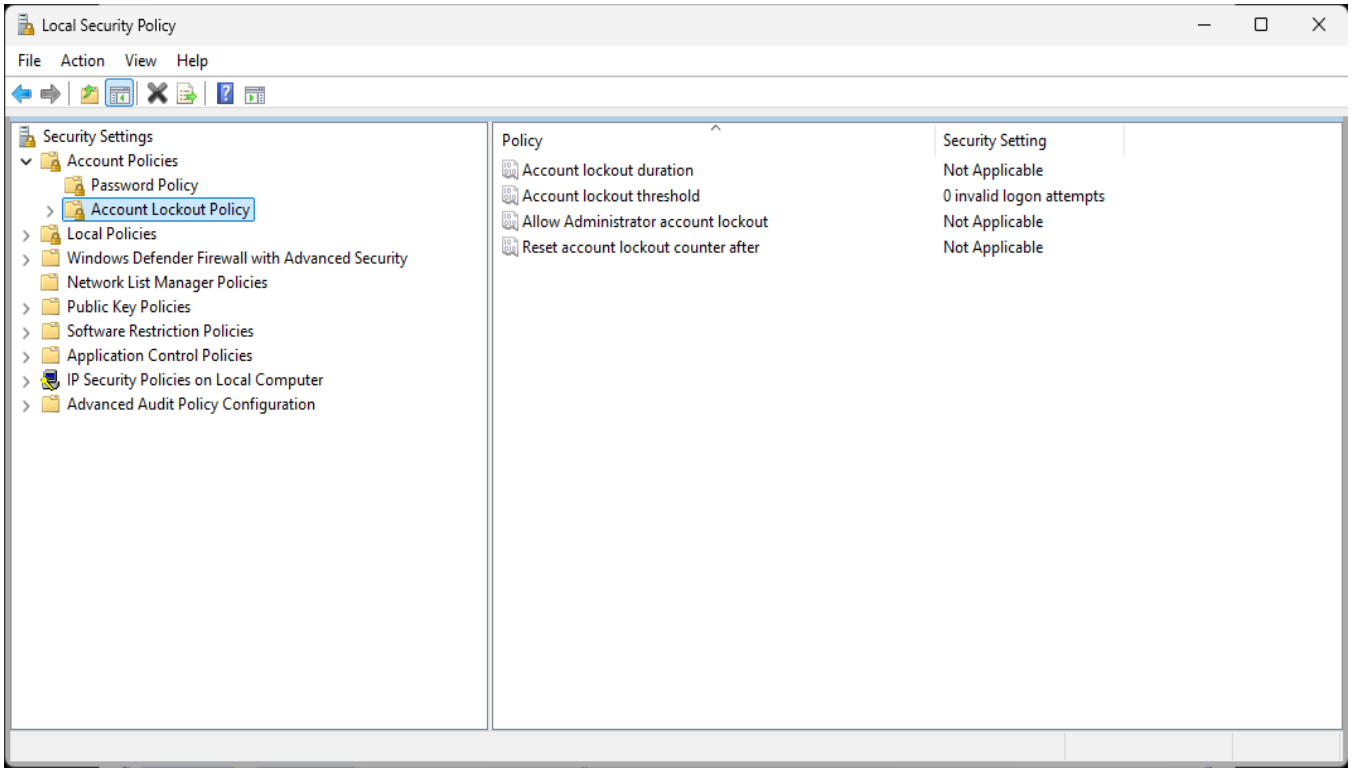
Auditing Security Settings

Place the screenshot of the password policy screen here



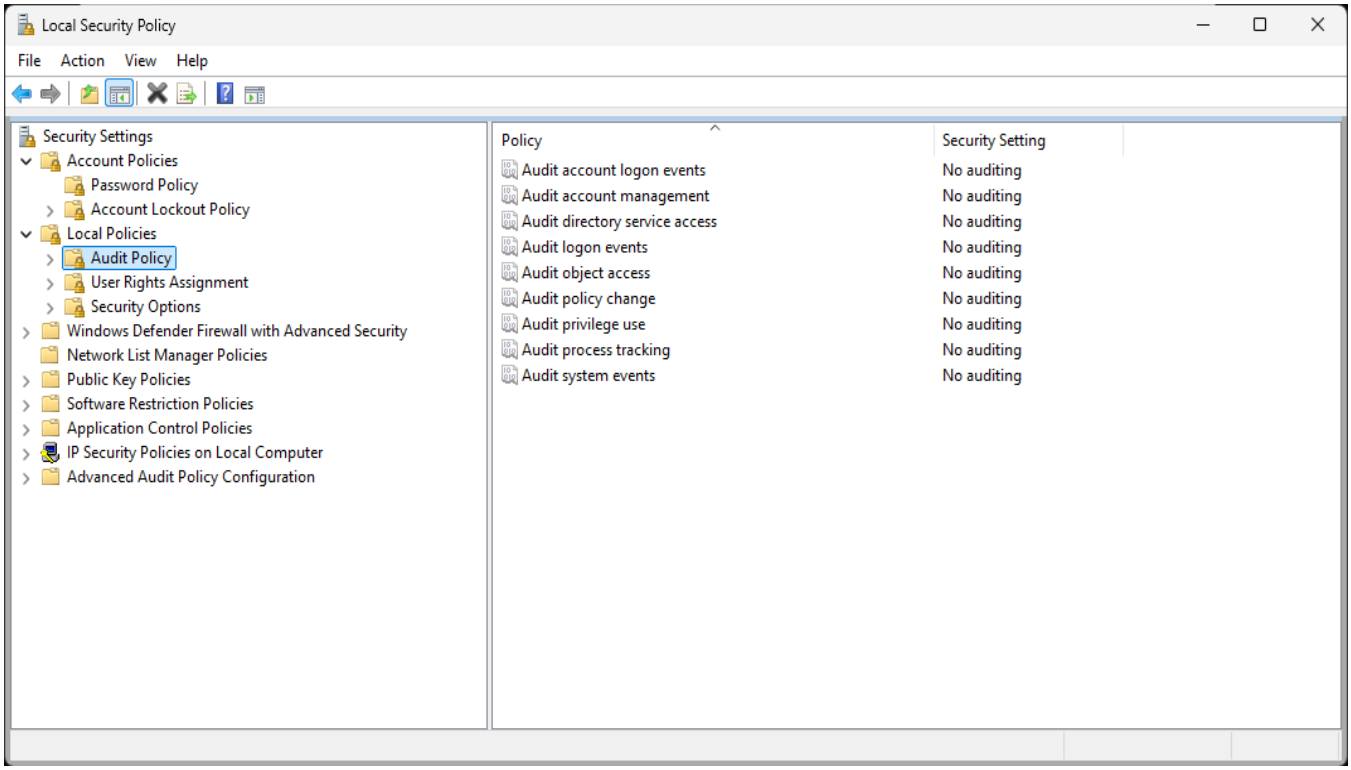
Auditing Security Settings

Place the screenshot of account lockout policy screen here



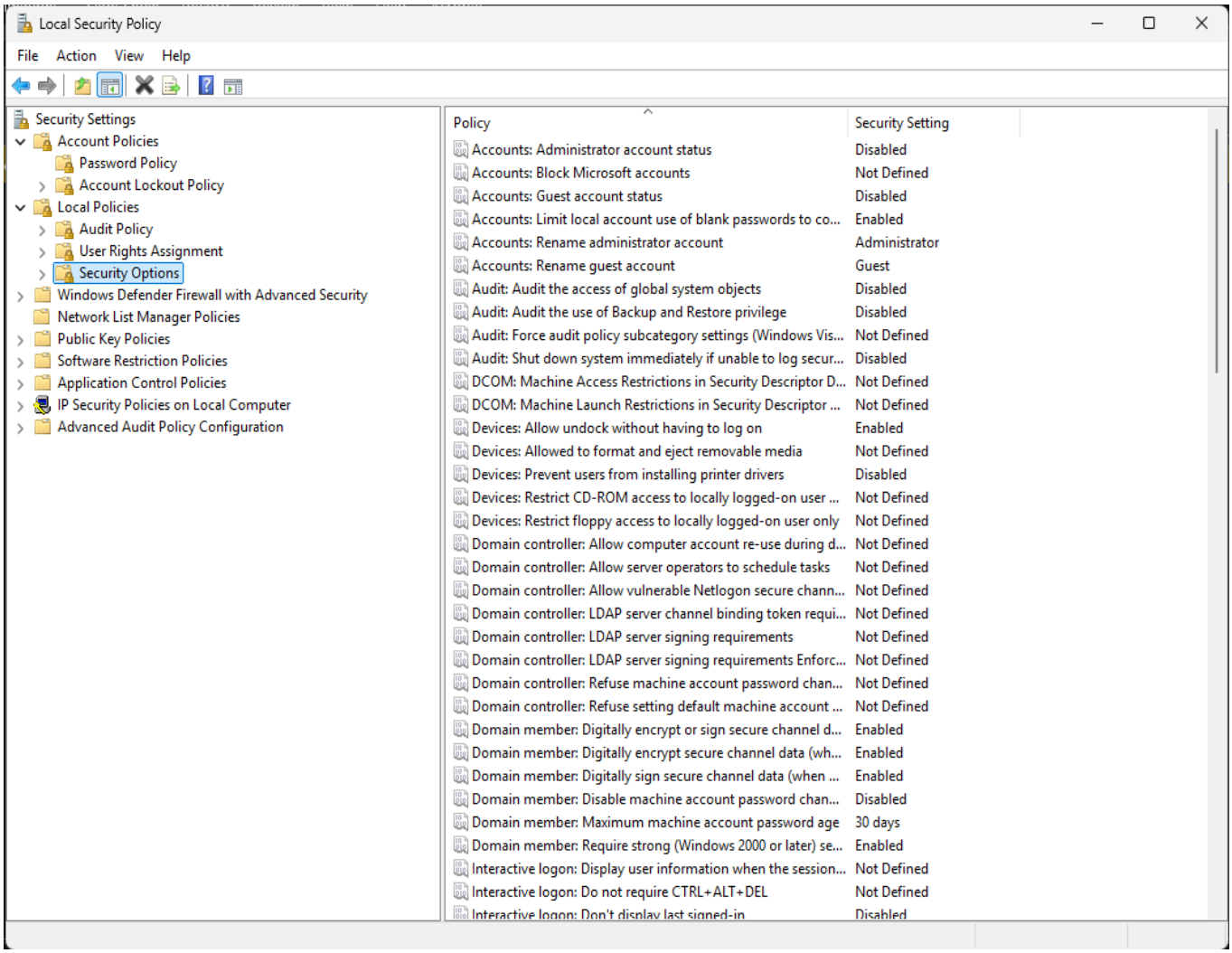
Auditing Security Settings

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. [Recommendation: (Enforce Strong Password Policy) Require passwords to be at least 10-12 characters long, include a mix of uppercase and lowercase letters, numbers and special characters. Set passwords to expire every 60-90 days and prevent password reuse for at least the previous 5 passwords.]
[Justification: A strong password policy significantly reduces the risk of successful brute force and credential stuffing attacks. Regular password changes further reduce the chance of compromised credentials being abused, while preventing reuse limits exposure from previously leaked passwords.]
2. [Recommendation: (Configure Strict Account Lockout Policy) Set the account lockout threshold to a maximum of 5 invalid login attempts, a lockout duration of at least 15 minutes, and a reset counter after 15 minutes.]
[Justification: This policy prevents attackers from attempting multiple password guesses (brute force attacks) on user accounts. Locking an account after consecutive failed attempts disrupts and deters unauthorized access attempts while limiting the risk of user lockout due to accidental mistakes.]
3. [Recommendation: (Enable Comprehensive Audit Logging) Enable auditing for logon events, account management, policy changes, privilege use and object access. Store audit logs securely and retain them for at least 6 months.]
[Justification: Detailed audit logs are vital for incident detection, investigation and regulatory compliance (such as SOX, HIPAA, or GDPR). They help identify suspicious activities, unauthorized changes, and enable rapid response to security incidents.]
4. [Recommendation: (Harden Security Options) Disable legacy and insecure protocols (such as SMB1, LM/NTLMv1), enforce Network Level Authentication (NLA) for RDP, and disable guest accounts. Set User Account Control (UAC) to require consent for elevated access.]
[Justification: Disabling insecure protocols and guest accounts minimizes attack surfaces and prevents exploitation of known vulnerabilities. Enforcing NLA and UAC enhances session security and reduces the risk of privilege escalation and unauthorized remote access.]

Section 4:
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 backups are recommended.]
Retention Period:	[Retain backups for at least 1 year.]
[Justification: Confidential data includes sensitive financial and personal information subject to strict regulations (like PCI DSS, GDPR, Bank Secrecy Act). Frequent backups minimize data loss risk and ensure quick recovery. Long retention supports regulatory audits and investigations, aligns with financial industry standards requiring multi-year retention periods.]	
Internal Data	
Backup Frequency:	[Daily backups are appropriate.]
Retention Period:	[Retain backups for around 90 days.]
[Justification: Internal business data requires protection to maintain continuity and audit readiness but changes less frequently than confidential data. Daily backups balance recovery needs and resource use. A 90-day retention window covers operational recovery and typical audit cycles without excessive storage costs.]	

Developing a Data Backup Strategy

Public Data	
Backup Frequency:	[Weekly backups is good, or as needed.]
Retention Period:	[Retain backups for at least 30 days.]
[ustification: Public data is low risk; loss does not have regulatory or operational impact. Weekly backups and shorter retention effectively optimize resources while providing enough recovery flexibility for accidental deletions or changes.]	

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 VirtualBox
- 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

As I'm using VMware Workstation, it doesn't provide a built-in backup feature. So I create a snapshot of the labVM as a backup.