

Student: Email:
Bradley Adams badams10@my.athens.edu

Time on Task: Progress:
3 hours, 18 minutes 100%

Report Generated: Saturday, November 9, 2024 at 3:01 PM

Guided Exercises

Part 1: Update the Information Security Policy Document

3. **Recommend** and **explain** four properties and any associated values.

1. Length

Explanation: Password length is the most critical factor in determining password strength. Longer passwords exponentially increase the number of possible combinations, making brute-force attacks significantly more difficult.

Recommendation: Aim for a minimum length of 12 characters, though 16 characters or more is recommended for high-security environments.

2. Complexity

Explanation: The inclusion of a mix of character types increases the password's measure of unpredictability, making it harder to guess or brute-force.

Recommendation: A strong password should include at least one uppercase letter, one lowercase letter, one number, and one special character.

3. Unpredictability

Explanation: Unpredictability focuses on avoiding common words, patterns, or phrases. Attackers often use dictionaries of common passwords, phrases, and even known patterns.

Recommendation: Use a password generator or choose a completely random combination of letters, numbers, and symbols. Avoid personal information and refrain from simple keyboard patterns.

4. Non-Reusability

Explanation: Reusing passwords across multiple accounts makes them vulnerable. Each account should have a unique password, which limits exposure if one password is compromised.

Recommendation: Use a unique password for each account managed through a password manager.

4. **Update** the existing password policy with an additional statement for each property.

2.2.1 Additional Statement: Employees must update their passwords every 90 days or immediately if they suspect any security compromise.

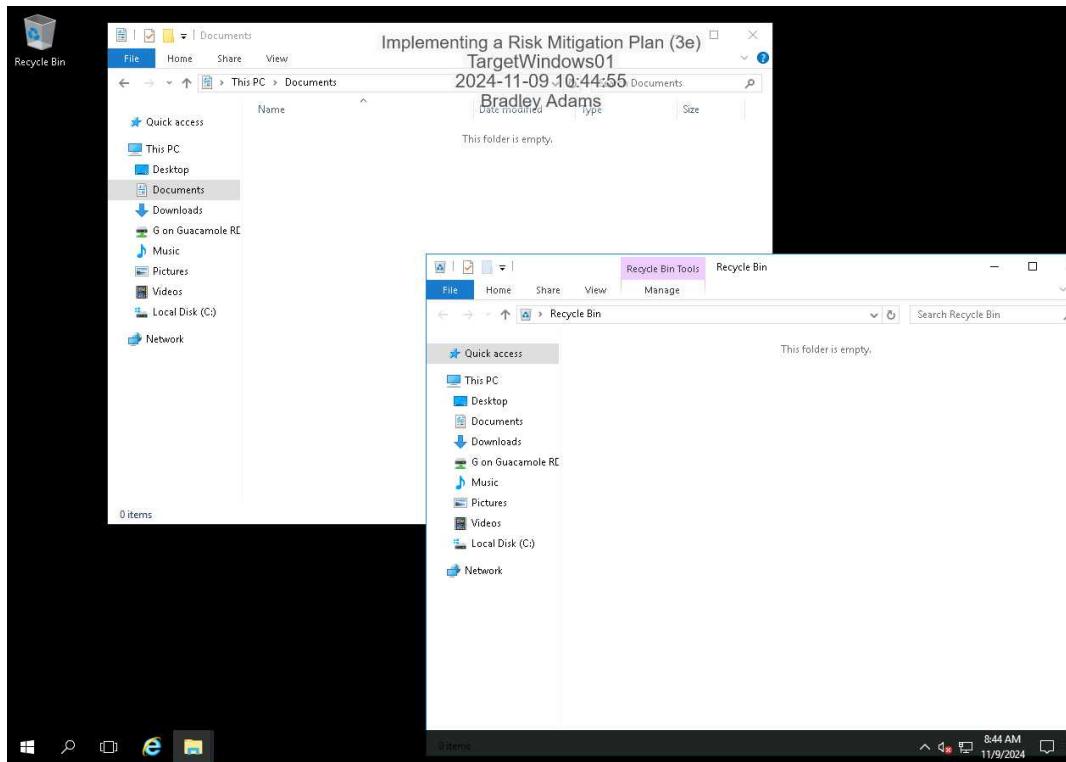
2.2.2 Additional Statement: Any access that requires shared credentials must be documented and approved through secure, temporary access solutions and management tools rather than by sharing individual passwords.

2.2.3 Additional Statement: Employees are encouraged to use an approved password manager to store and manage complex passwords securely.

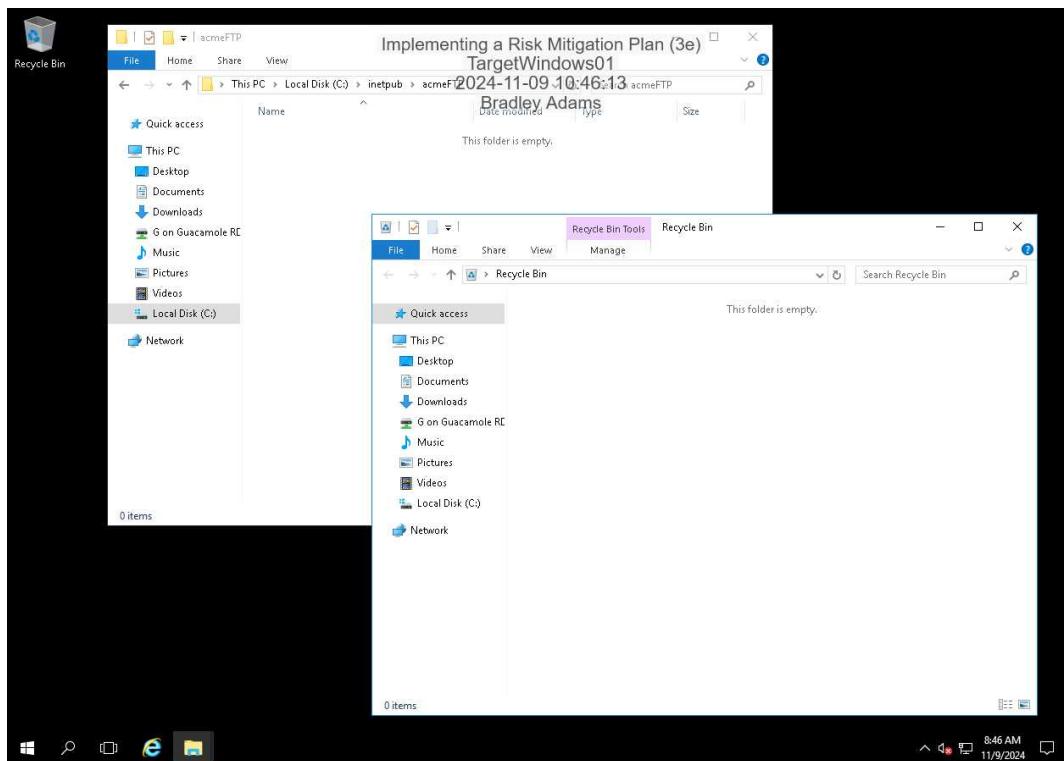
2.2.4 Additional Statement: Employees are required to set strong, unique passwords specific to Acme's systems and should avoid using personal information in their passwords.

Part 2: Sanitize a Windows Server

7. **Make a screen capture showing the empty Documents folder and empty Recycle Bin icon.**



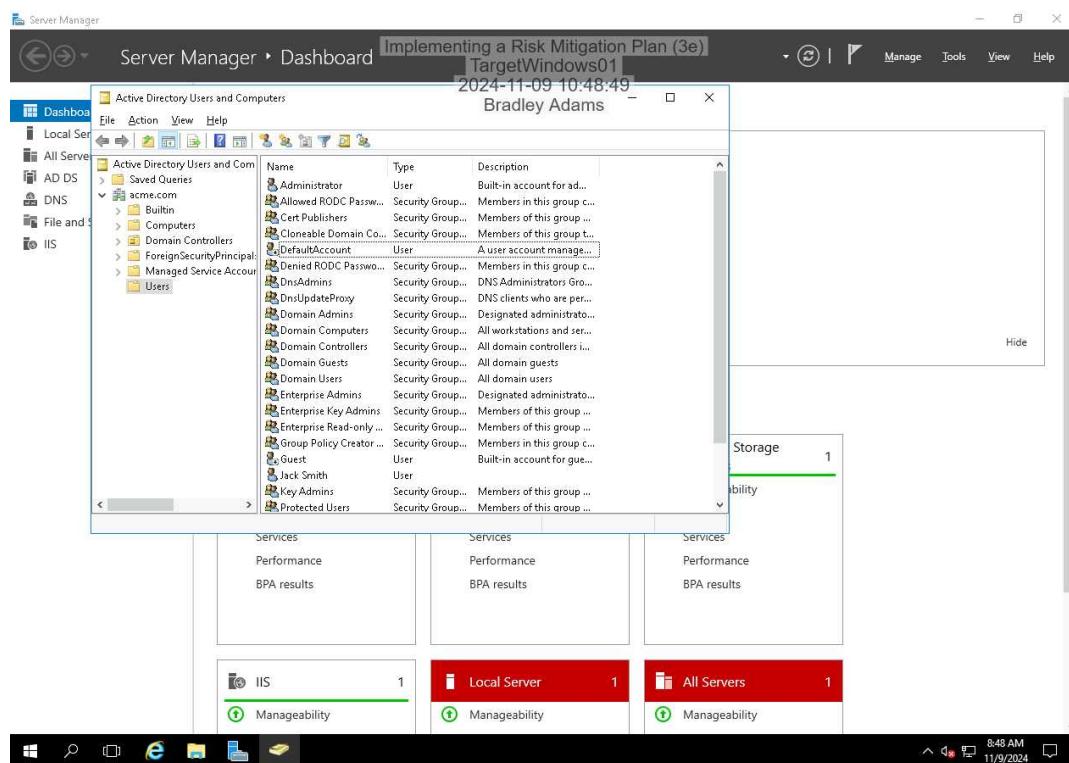
12. Make a screen capture showing the empty acmeFTP folder and empty Recycle Bin icon.



Implementing a Risk Mitigation Plan (3e)

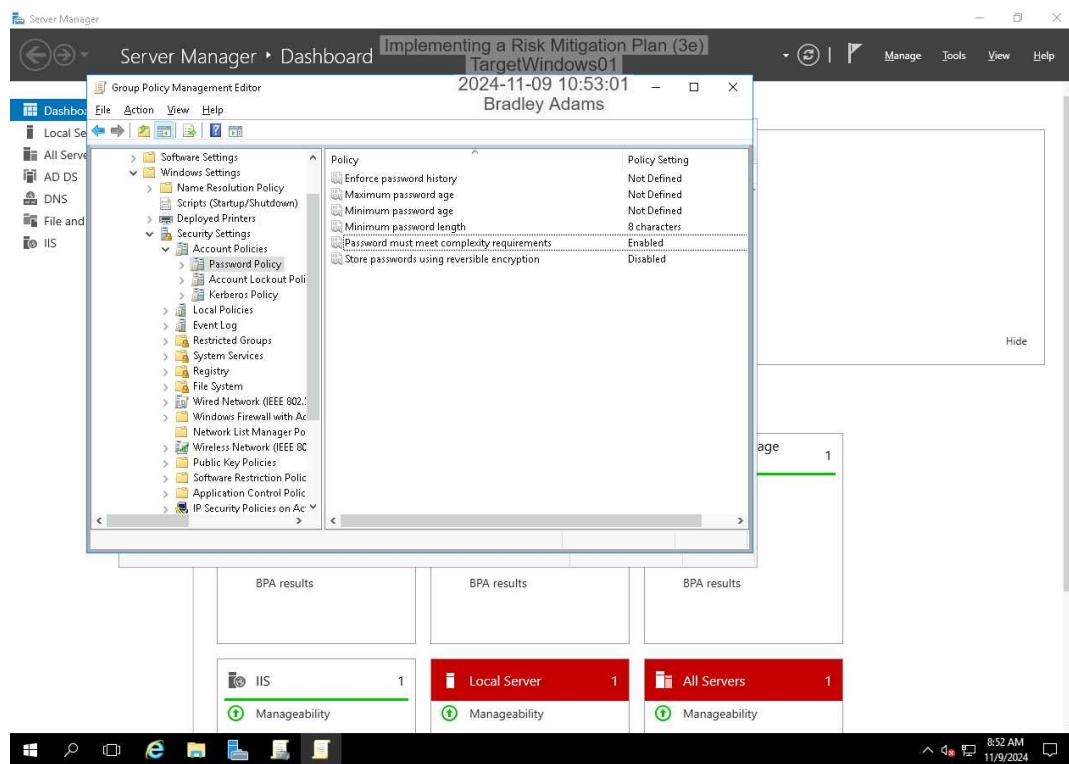
Managing Risk in Information Systems, Third Edition - Lab 08

22. Make a screen capture showing the Active Directory Users and Computers console without the Database_Test user.



Part 3: Update the Active Directory Password Policy

11. Make a screen capture showing the updated password policy.

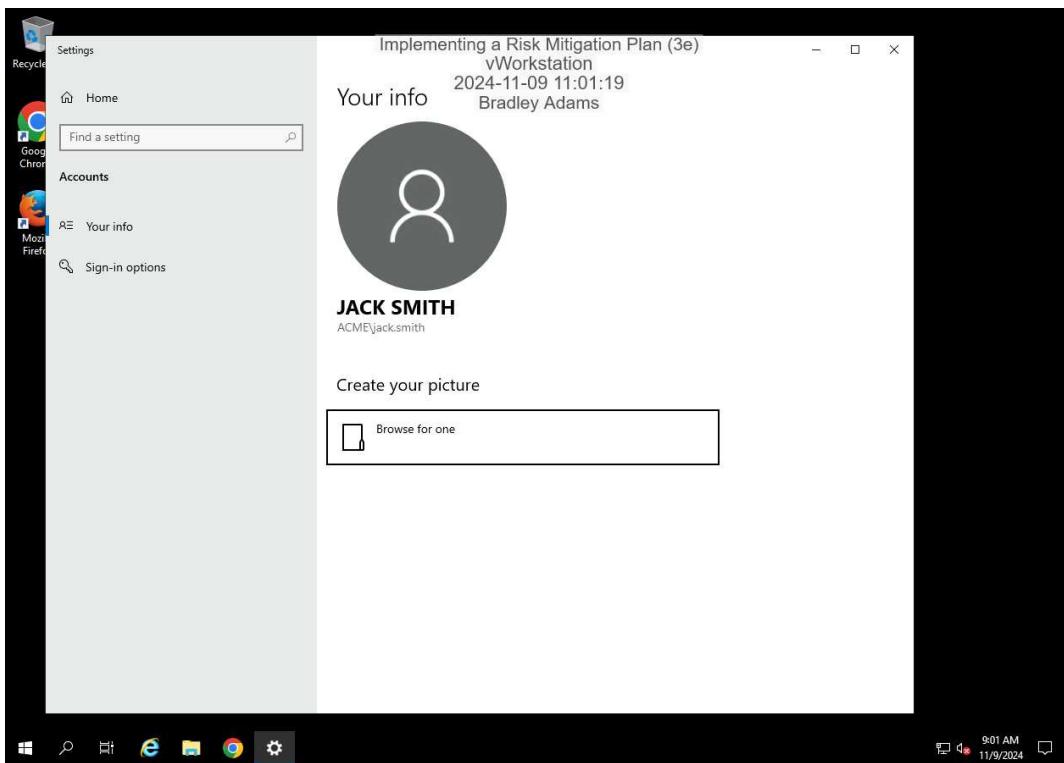


Part 4: Change a User Password

12. Record the new password that you used.

Nxh(q3Dc

14. Make a screen capture showing the **Jack Smith** account logged in on the vWorkstation.



Challenge Exercises

Part 1: Define a Security Policy for Handling Sensitive Information

Create one or more clauses for each policy requirement.

3.3 Handling Sensitive Information

3.3.1 Responsibilities

a. Users

- Users are responsible for safeguarding sensitive data and storing all sensitive data on approved encrypted storage solutions.
- Users are to promptly report any incident in violation of policy to their immediate supervisor.
- b. System and Security Administrators
- System Administrators and Security Administrators are responsible for implementing and maintaining secure storage systems.
- Security Administrators must perform regular audits to identify and report risks associated with improper storage of sensitive data.
- System Administrators and Security Administrators will provide users with educational information and guide them on proper data storage practices when they request it or in reference to a violation of policy.

3.3.2 Prohibition on Storing Sensitive Data in Insecure Locations

- Users are prohibited from storing sensitive data on non-secure media.
- Sensitive data must only be stored on devices, drives, or any other media approved by Acme's Information Security team.

3.3.3 Disciplinary Actions for Policy Violations

First Violation: A documented warning and mandatory training on secure data practices and policy.

Second Violation: Temporary suspension of system access and a comprehensive review with the security team and supervision.

Subsequent Violations: Possible termination of employment or access revocation.

-In cases where policy violations result in the actual or potential exposure of sensitive data, Acme Corporation may take further legal action based on the level of negligence or intent involved.

Part 2: Map Your Actions to the ISO/IEC 27002 Information Security Controls

Describe what you have already done in response to four of the security controls.

Information Security policies: Created and updated a Password policy and a Handling Sensitive Information policy

Allocation of information security responsibilities: Handling Sensitive Information policy assigns and outlines roles and responsibilities for users and security and system administrators.

Protection of organizational records: Handling Sensitive Information policy further protects those records labeled sensitive.

Information security awareness, education, and training: Both the Password Policy and the Handling Sensitive Information policy provides for requirements on education and training.

Identify the five security controls that are not applicable to this case.

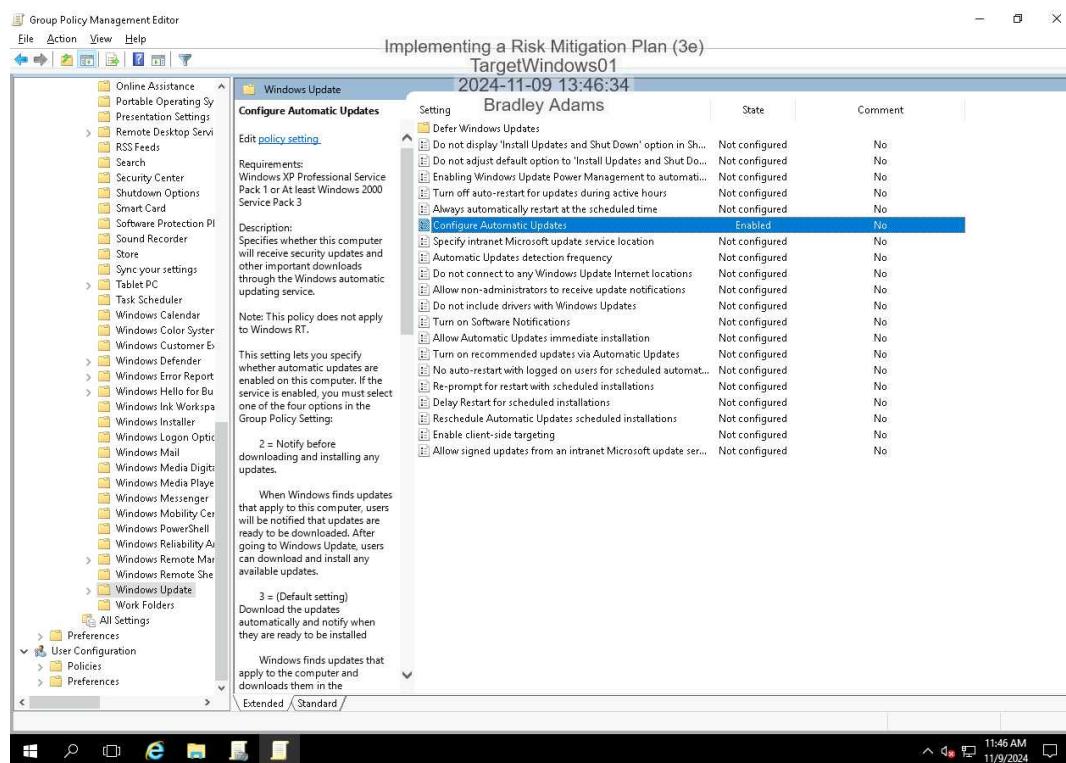
Business continuity management
Correct data processing
Enforce intellectual property rights
Technical vulnerability management
Management of information security incidents

Describe what you could do to implement the remaining security control.

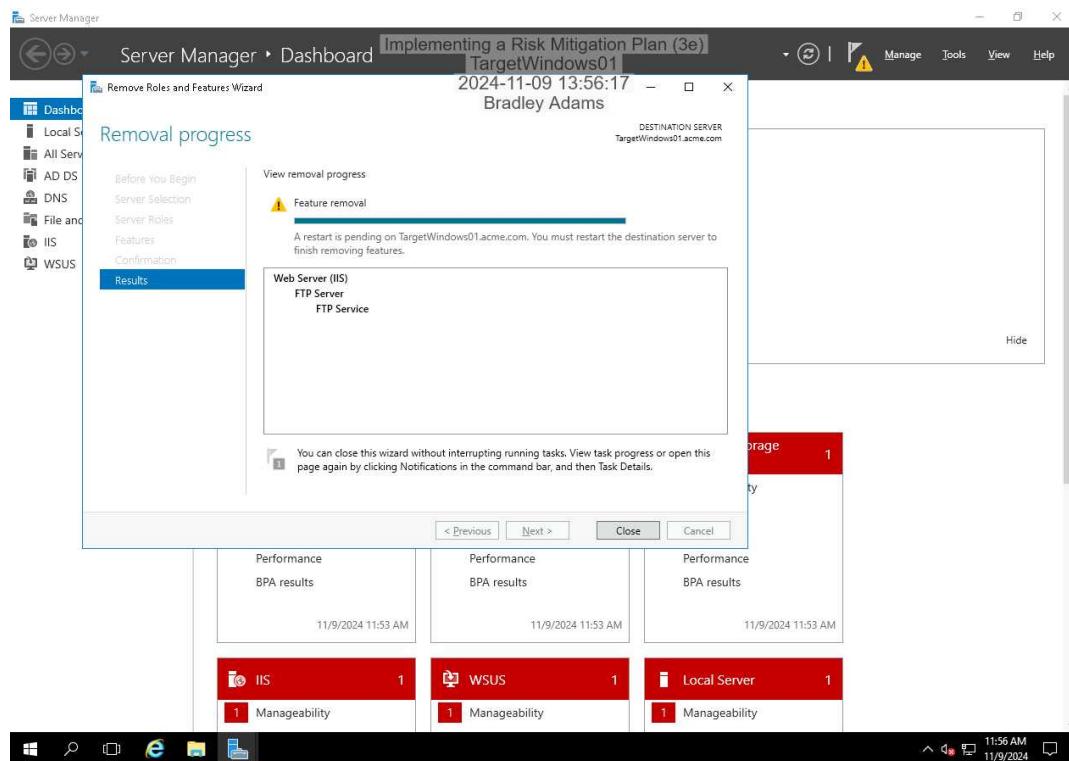
Data protection and privacy of personal information: password policy does not allow for any personal information to be used to create a password and the Handling Sensitive Information policy could be updated to address PII of users and employees.

Part 3: Harden TargetWindows01

Make a screen capture showing the activated Windows Update service.



Make a screen capture showing the disabled Microsoft FTP service.



Implementing a Risk Mitigation Plan (3e)

Managing Risk in Information Systems, Third Edition - Lab 08

Make a screen capture showing the **uninstalled third-party management tool** that you located.

