Developing a Risk Mitigation Plan (3e)

Managing Risk in Information Systems, Third Edition - Lab 07

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

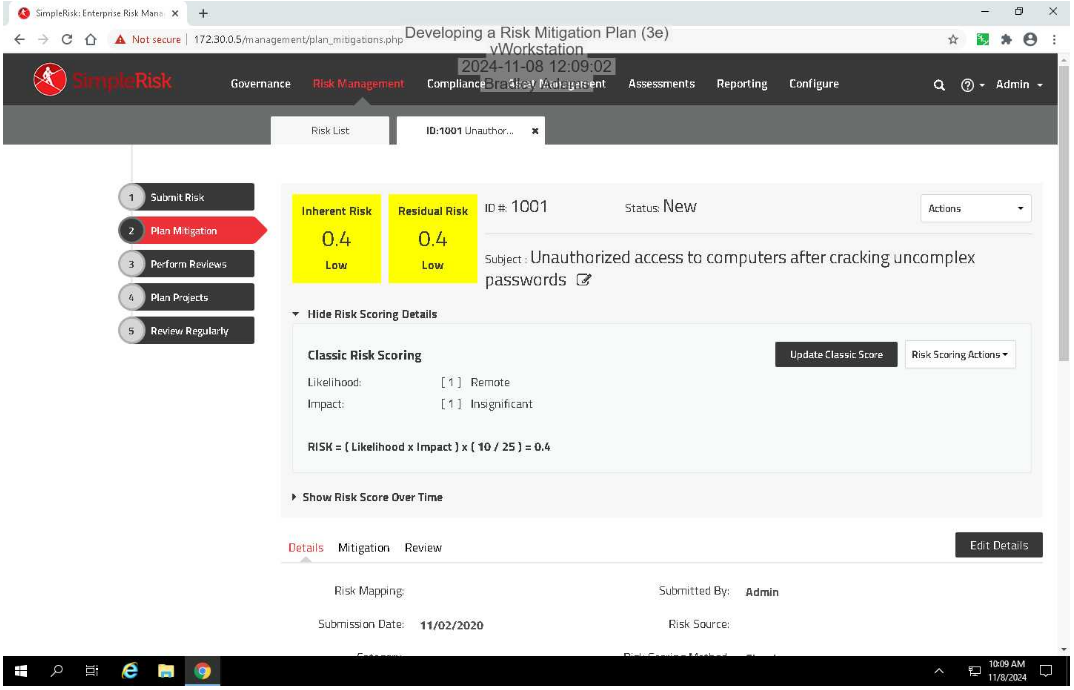
Time on Task:	Progress:
1 hour, 27 minutes	100%

Report Generated: Friday, November 8, 2024 at 2:29 PM

Guided Exercises

Part 1: Prepare a Risk Mitigation Plan

13. **Make a screen capture** showing the **updated inherent risk value**.



Developing a Risk Mitigation Plan (3e)
vWorkstation
2024-11-08 12:09:02
Bradley Adams

Inherent Risk 0.4 Low

Residual Risk 0.4 Low

ID #: 1001

Status: New

Subject : Unauthorized access to computers after cracking uncomplex passwords

Classic Risk Scoring

Likelihood: [1] Remote

Impact: [1] Insignificant

RISK = (Likelihood x Impact) x (10 / 25) = 0.4

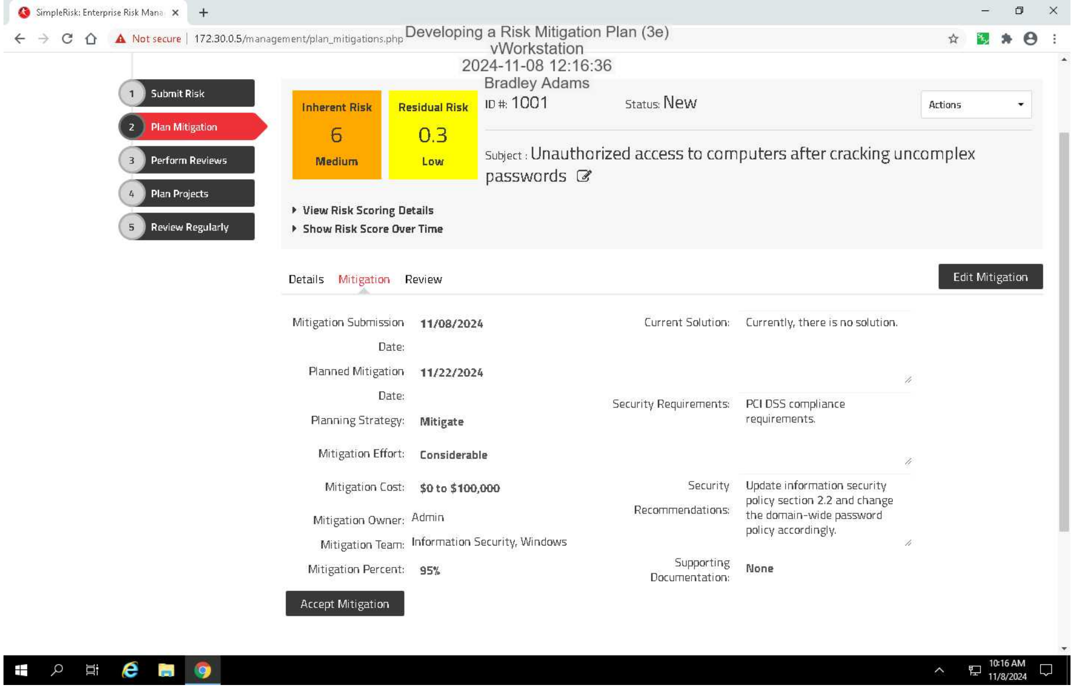
Risk Mapping:

Submitted By: Admin

Submission Date: 11/02/2020

Risk Source:

33. **Make a screen capture** showing the **updated Residual Risk value.**



Developing a Risk Mitigation Plan (3e)
vWorkstation
2024-11-08 12:16:36
Bradley Adams

SimpleRisk: Enterprise Risk Mana
Not secure | 172.30.0.5/management/plan_mitigations.php

Inherent Risk 6 Medium

Residual Risk 0.3 Low

ID #: 1001 Status: New

Subject : Unauthorized access to computers after cracking uncomplex passwords

Mitigation Submission Date: 11/08/2024

Planned Mitigation Date: 11/22/2024

Planning Strategy: Mitigate

Mitigation Effort: Considerable

Mitigation Cost: $0 to $100,000

Mitigation Owner: Admin

Mitigation Team: Information Security, Windows

Mitigation Percent: 95%

Current Solution: Currently, there is no solution.

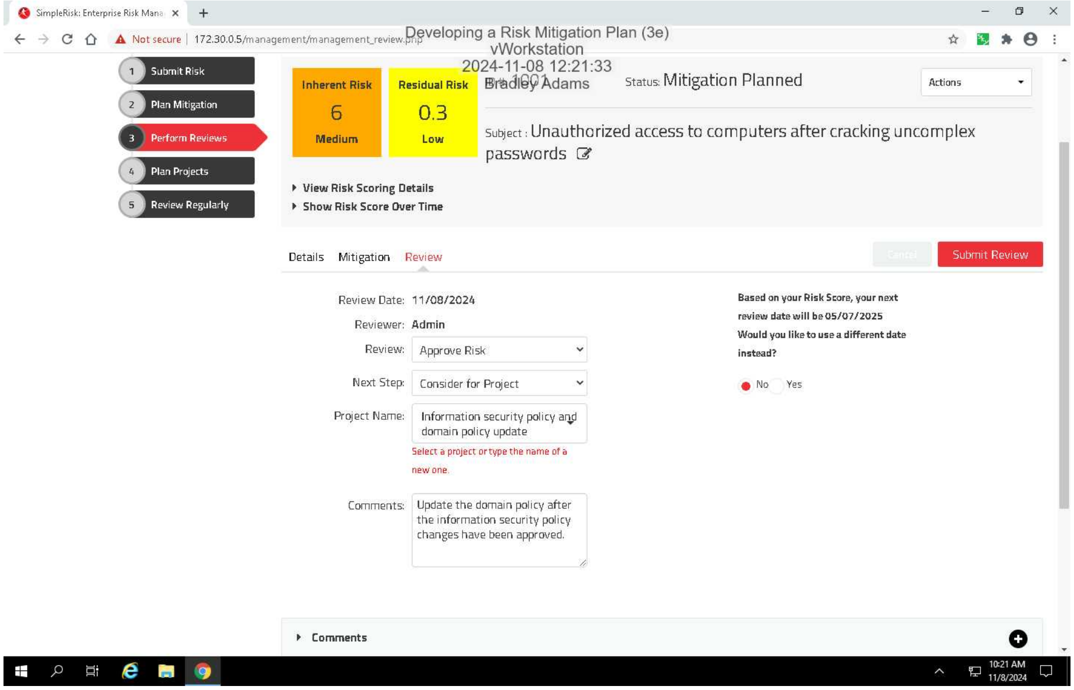
Security Requirements: PCI DSS compliance requirements.

Security Recommendations: Update information security policy section 2.2 and change the domain-wide password policy accordingly.

Supporting Documentation: None

Part 2: Conduct a Management Review

9. **Make a screen capture** showing the **completed Mitigation Review page**.



Developing a Risk Mitigation Plan (3e)
vWorkstation
2024-11-08 12:21:33
Bradley Adams

SimpleRisk: Enterprise Risk Mana
Not secure | 172.30.0.5/management/management_review.php

Inherent Risk 6 Medium

Residual Risk 0.3 Low

ID #: 1001 Status: Mitigation Planned

Subject : Unauthorized access to computers after cracking uncomplex passwords

Review Date: 11/08/2024

Reviewer: Admin

Review: Approve Risk

Next Step: Consider for Project

Project Name: Information security policy and domain policy update

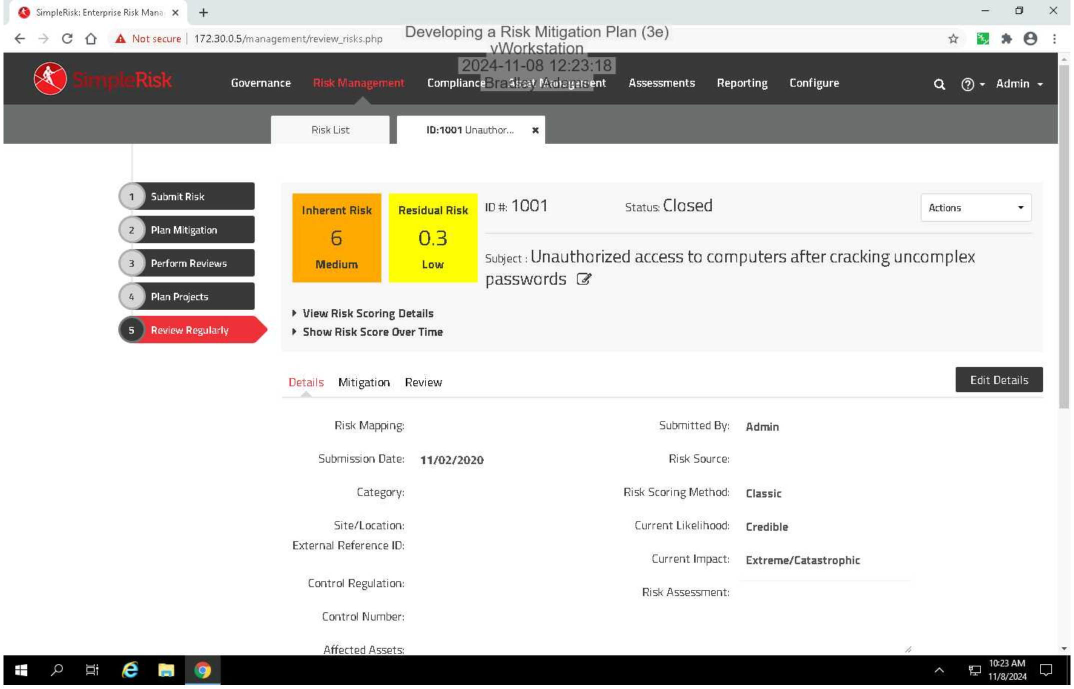
Select a project or type the name of a new one.

Comments: Update the domain policy after the information security policy changes have been approved.

Based on your Risk Score, your next review date will be 05/07/2025
Would you like to use a different date instead?

● No ○ Yes

15. **Make a screen capture** showing the **closed risk**.



Inherent Risk 6 Medium

Residual Risk 0.3 Low

ID #: 1001

Status: Closed

Subject : Unauthorized access to computers after cracking uncomplex passwords

Risk Mapping:

Submission Date: 11/02/2020

Category:

Site/Location:

External Reference ID:

Control Regulation:

Control Number:

Affected Assets:

Submitted By: Admin

Risk Source:

Risk Scoring Method: Classic

Current Likelihood: Credible

Current Impact: Extreme/Catastrophic

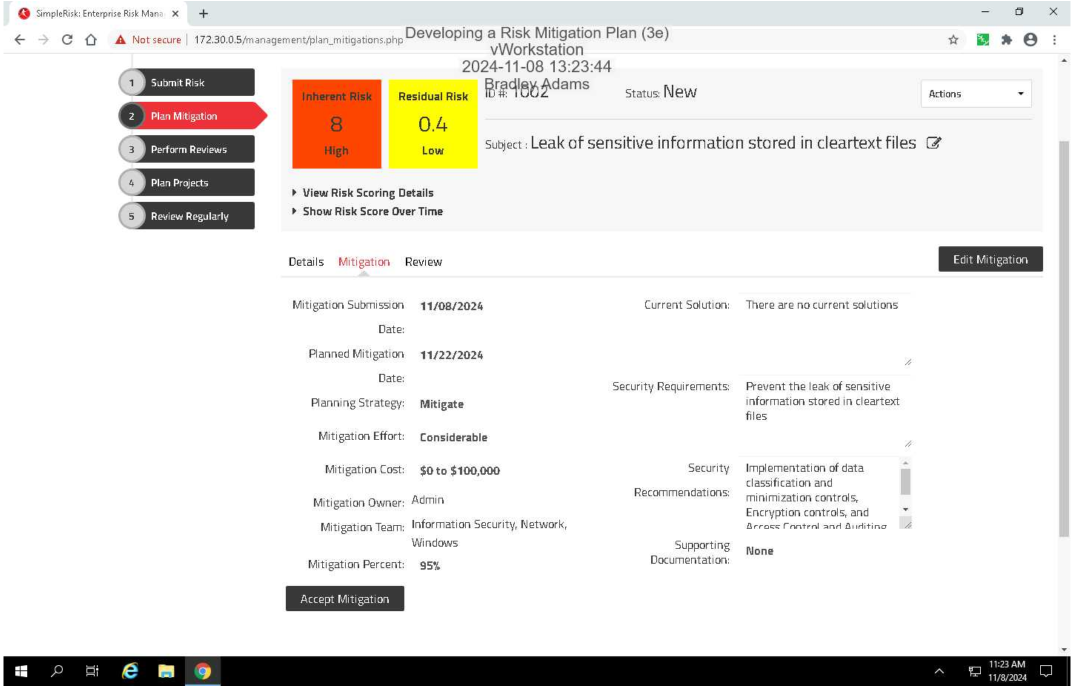
Risk Assessment:

Challenge Exercise

Define three security controls designed to mitigate the risk associated with a recent leak of sensitive information that was stored in cleartext files.

Asset Value: Organizational Level
Security Control = Data Classification and Minimization
-Strategic control would be a policy that eliminates outdated or unnecessary sensitive data
-Tactical control would be an automated tool to classify sensitive data
Vulnerability severity: Mission/Business Process Level
Security Control = Encryption
-Strategic control would be a policy mandating an encryption standard
-Tactical control could be a DLP(data loss prevention) solution to flag plaintext files
Threat Impact: Information System Level
Security Control = Access Control and Auditing
-Strategic control is to establish RBAC policies, access based on need-to-know, regular reviews
-Tactical control could be a SIEM monitoring access behavior with alerts

Make a screen capture showing your **completed Risk Mitigation plan in SimpleRisk**.



Developing a Risk Mitigation Plan (3e)
vWorkstation
2024-11-08 13:23:44
Bradley Adams

Inherent Risk: 8 High

Residual Risk: 0.4 Low

ID #: 1002

Status: New

Subject : Leak of sensitive information stored in cleartext files

Mitigation Submission Date: 11/08/2024

Planned Mitigation Date: 11/22/2024

Planning Strategy: Mitigate

Mitigation Effort: Considerable

Mitigation Cost: $0 to $100,000

Mitigation Owner: Admin

Mitigation Team: Information Security, Network, Windows

Mitigation Percent: 95%

Current Solution: There are no current solutions

Security Requirements: Prevent the leak of sensitive information stored in cleartext files

Security Recommendations: Implementation of data classification and minimization controls, Encryption controls, and Access Control and Auditing

Supporting Documentation: None