# Conducting a PCI DSS Compliance Review (3e)

Managing Risk in Information Systems, Third Edition - Lab 02

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

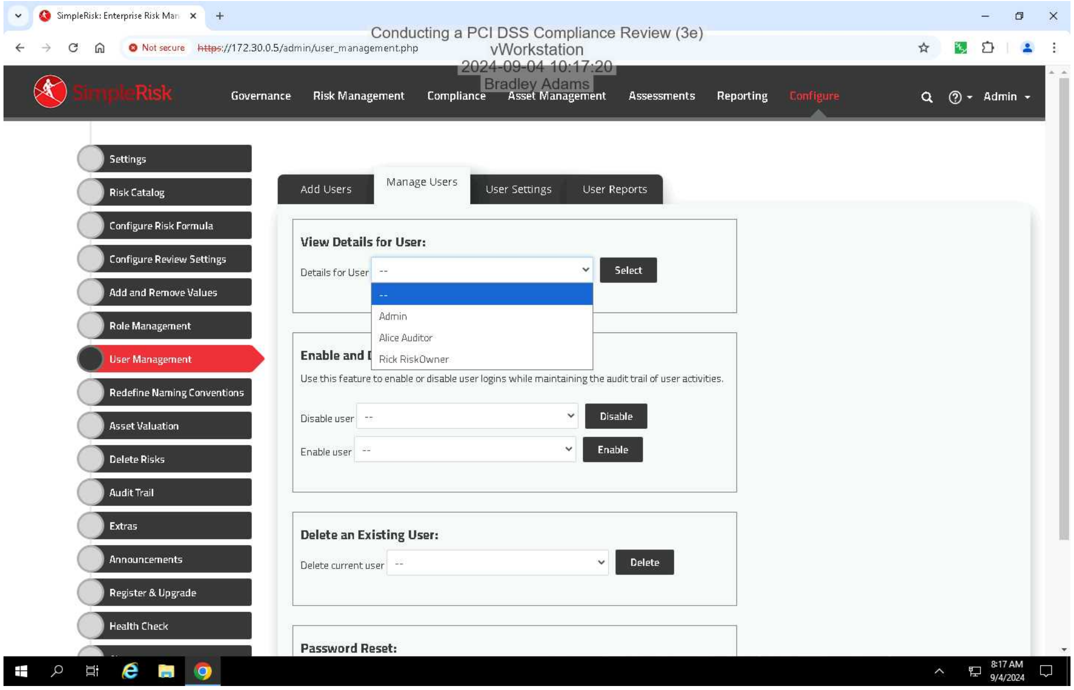
| | |
|---|---|
| Time on Task: | Progress: |
| 1 hour, 27 minutes | 100% |

Report Generated: Wednesday, September 4, 2024 at 12:21 PM

# Guided Exercises

## Part 1: Create User Roles and Accounts

21. **Make a screen capture** showing the **two new user accounts in SimpleRisk**.



Conducting a PCI DSS Compliance Review (3e)
vWorkstation
2024-09-04 10:17:20
Bradley Adams

https://172.30.0.5/admin/user_management.php

View Details for User:

Details for User: --

- --
- Admin
- Alice Auditor
- Rick RiskOwner

Enable and Disable

Use this feature to enable or disable user logins while maintaining the audit trail of user activities.

Disable user --

Enable user --

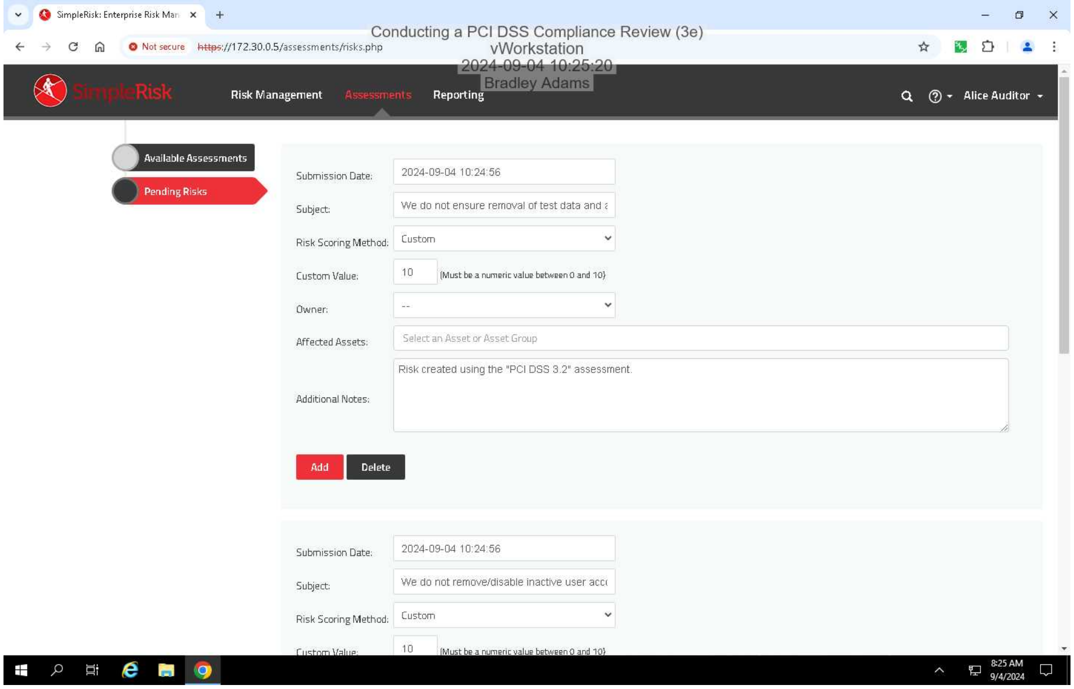
Delete an Existing User:

Delete current user --

Password Reset:

## Part 2: Identify Instances of Noncompliance

11. **Make a screen capture** showing the **first risk entry on the Pending Risks page.**

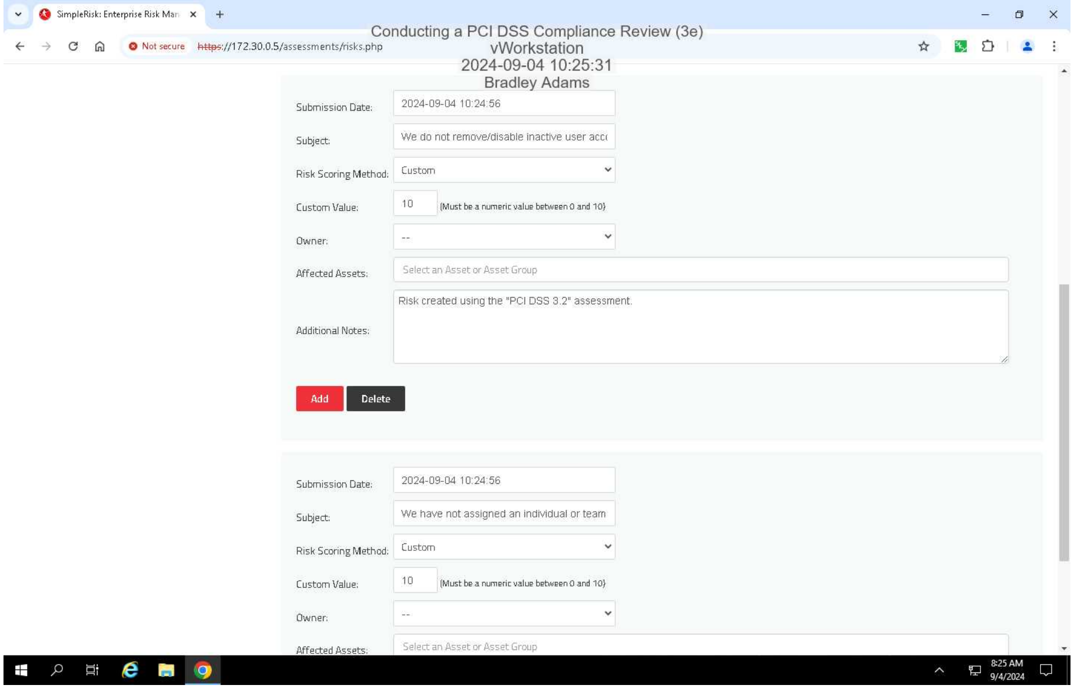


Conducting a PCI DSS Compliance Review (3e)
vWorkstation
2024-09-04 10:25:20
Bradley Adams

Submission Date: 2024-09-04 10:24:56
Subject: We do not ensure removal of test data and a
Risk Scoring Method: Custom
Custom Value: 10 (Must be a numeric value between 0 and 10)
Owner: --
Affected Assets: Select an Asset or Asset Group
Additional Notes: Risk created using the "PCI DSS 3.2" assessment.
Add Delete

Submission Date: 2024-09-04 10:24:56
Subject: We do not remove/disable inactive user acc
Risk Scoring Method: Custom
Custom Value: 10 (Must be a numeric value between 0 and 10)

12. **Make a screen capture** showing the **second risk entry on the Pending Risks page**.

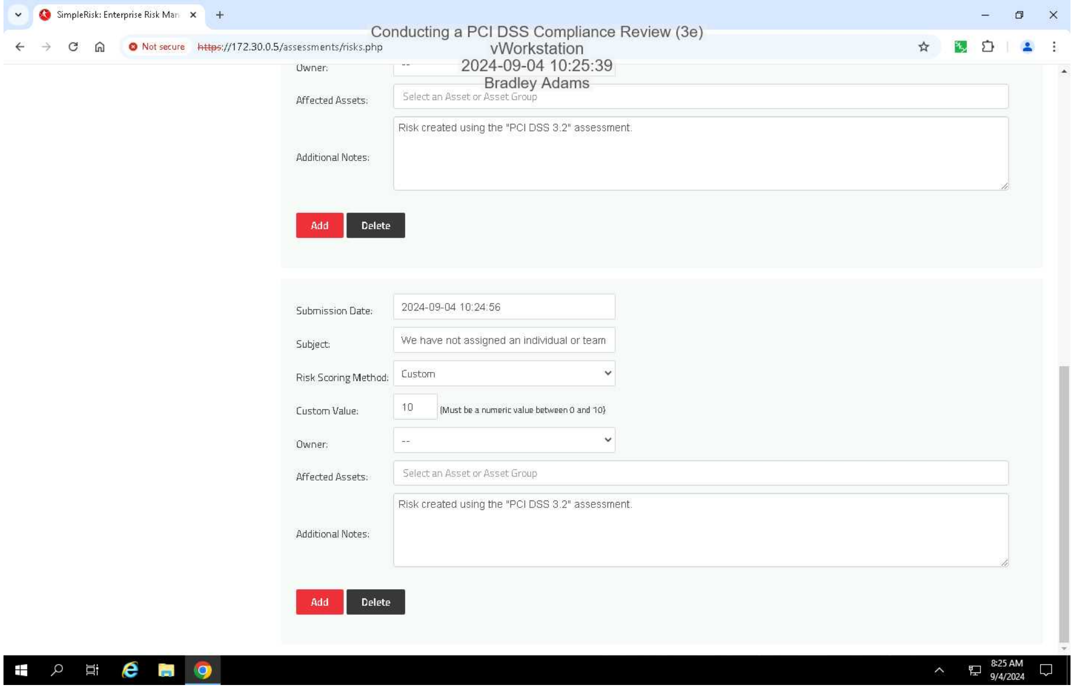

SimpleRisk: Enterprise Risk Man
Not secure
https://172.30.0.5/assessments/risks.php
8:25 AM
9/4/2024

Conducting a PCI DSS Compliance Review (3e)
vWorkstation
2024-09-04 10:25:31
Bradley Adams

Submission Date: 2024-09-04 10:24:56
Subject: We do not remove/disable inactive user acc
Risk Scoring Method: Custom
Custom Value: 10 (Must be a numeric value between 0 and 10)
Owner: --
Affected Assets: Select an Asset or Asset Group
Additional Notes: Risk created using the "PCI DSS 3.2" assessment.
Add Delete

Submission Date: 2024-09-04 10:24:56
Subject: We have not assigned an individual or team
Risk Scoring Method: Custom
Custom Value: 10 (Must be a numeric value between 0 and 10)
Owner: --
Affected Assets: Select an Asset or Asset Group

13. **Make a screen capture** showing the **third risk entry on the Pending Risks page**.



SimpleRisk: Enterprise Risk Man
Not secure
https://172.30.0.5/assessments/risks.php
Conducting a PCI DSS Compliance Review (3e)
vWorkstation
2024-09-04 10:25:39
Bradley Adams
Add
Delete
Add
Delete
8:25 AM
9/4/2024

Owner: --

Affected Assets: Select an Asset or Asset Group

Additional Notes: Risk created using the "PCI DSS 3.2" assessment.

Submission Date: 2024-09-04 10:24:56

Subject: We have not assigned an individual or team

Risk Scoring Method: Custom

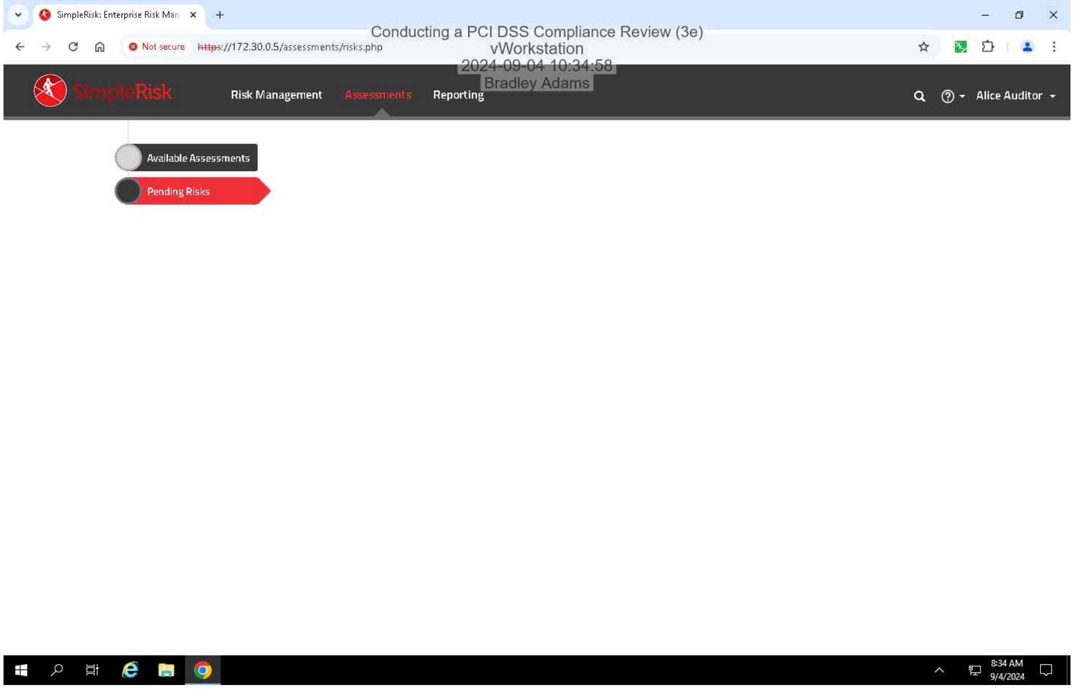
Custom Value: 10 (Must be a numeric value between 0 and 10)

Owner: --

Affected Assets: Select an Asset or Asset Group

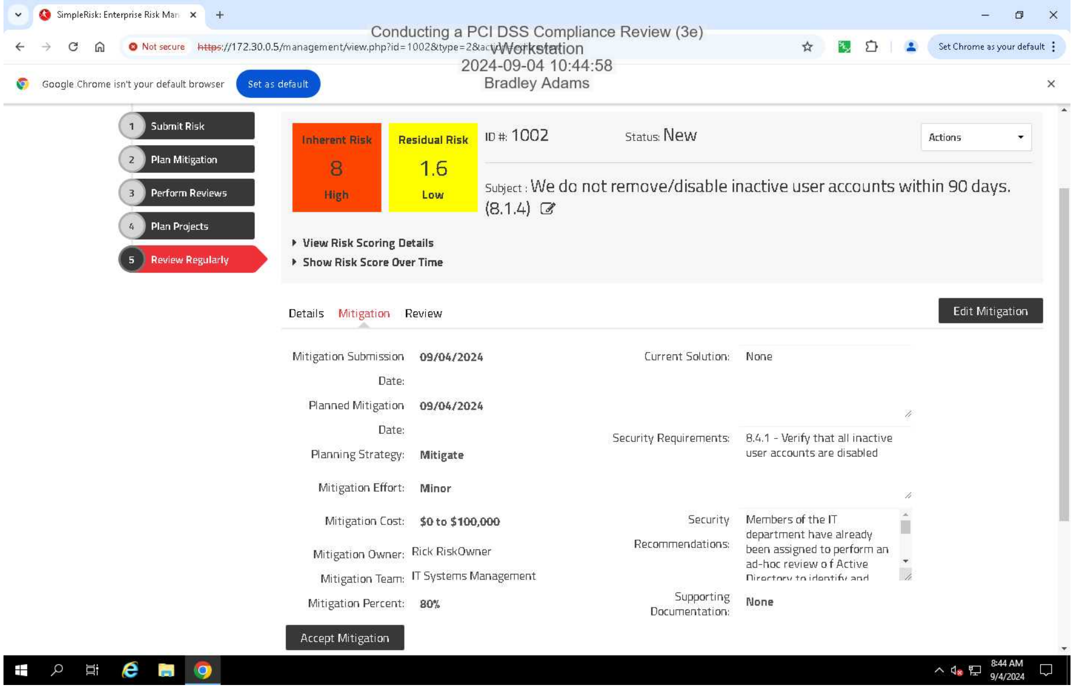
Additional Notes: Risk created using the "PCI DSS 3.2" assessment.

32. **Make a screen capture** showing the **empty Pending Risks page**.



## Part 3: Review Risks and Set Mitigation Actions

7. **Make a screen capture** showing the **inherent and residual risk levels**.


SimpleRisk: Enterprise Risk Man
Not secure
https://172.30.0.5/management/view.php?id=1002&type=2&ac
Set Chrome as your default
Google Chrome isn't your default browser
Set as default
1 Submit Risk
2 Plan Mitigation
3 Perform Reviews
4 Plan Projects
5 Review Regularly
Actions
View Risk Scoring Details
Show Risk Score Over Time
Details
Mitigation
Review
Edit Mitigation
Accept Mitigation
8:44 AM
9/4/2024

Conducting a PCI DSS Compliance Review (3e)
vWorkstation
2024-09-04 10:44:58
Bradley Adams

Inherent Risk 8 High

Residual Risk 1.6 Low

ID #: 1002 Status: New

Subject : We do not remove/disable inactive user accounts within 90 days. (8.1.4)

Mitigation Submission Date: 09/04/2024

Planned Mitigation Date: 09/04/2024

Planning Strategy: Mitigate

Mitigation Effort: Minor

Mitigation Cost: $0 to $100,000

Mitigation Owner: Rick RiskOwner

Mitigation Team: IT Systems Management

Mitigation Percent: 80%

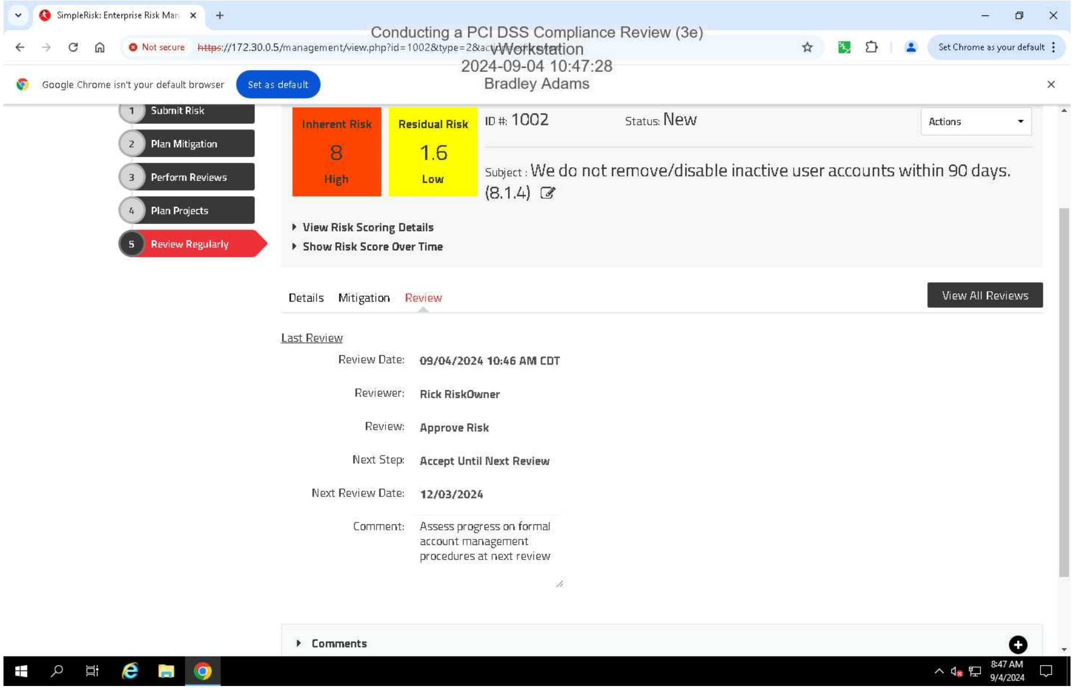
Current Solution: None

Security Requirements: 8.4.1 - Verify that all inactive user accounts are disabled

Security Recommendations: Members of the IT department have already been assigned to perform an ad-hoc review o f Active Directory to identify and

Supporting Documentation: None

11. **Make a screen capture** showing the **completed Review tab for Risk 1002**.


SimpleRisk: Enterprise Risk Man
Not secure
https://172.30.0.5/management/view.php?id=1002&type=2&ac
Set Chrome as your default
Google Chrome isn't your default browser
Set as default
1 Submit Risk
2 Plan Mitigation
3 Perform Reviews
4 Plan Projects
5 Review Regularly
Actions
View Risk Scoring Details
Show Risk Score Over Time
Details
Mitigation
Review
View All Reviews
Comments
8:47 AM
9/4/2024

Conducting a PCI DSS Compliance Review (3e)
vWorkstation
2024-09-04 10:47:28
Bradley Adams

Inherent Risk 8 High

Residual Risk 1.6 Low

ID #: 1002 Status: New

Subject : We do not remove/disable inactive user accounts within 90 days. (8.1.4)

Last Review

Review Date: 09/04/2024 10:46 AM CDT

Reviewer: Rick RiskOwner

Review: Approve Risk

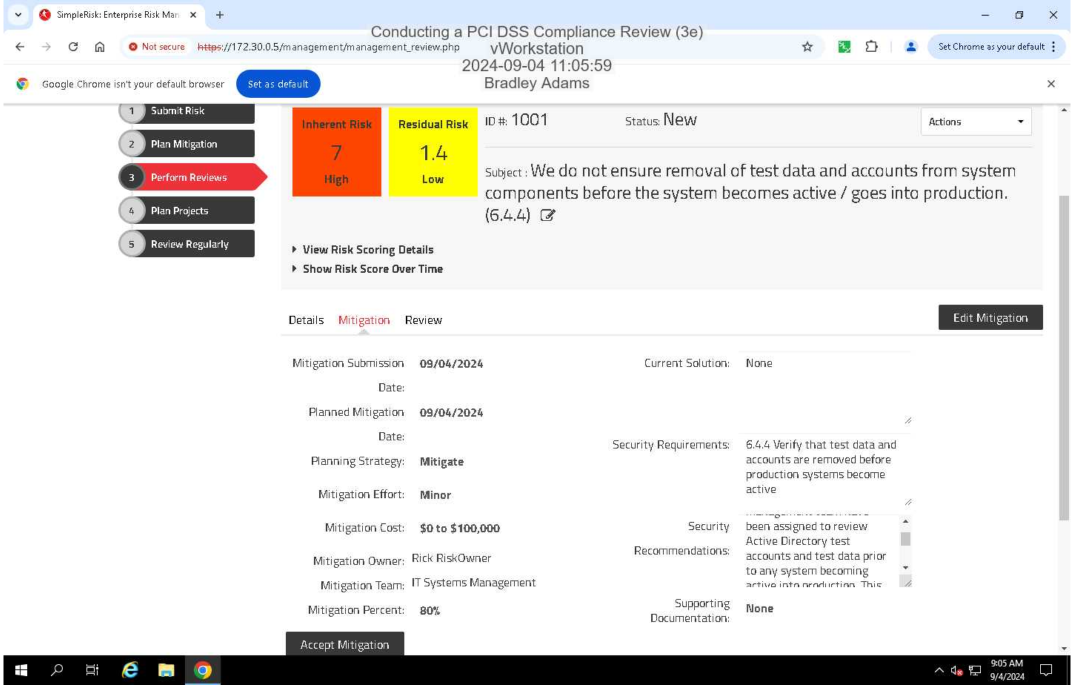
Next Step: Accept Until Next Review

Next Review Date: 12/03/2024

Comment: Assess progress on formal account management procedures at next review

# Challenge Exercise

**Make a screen capture** showing the **completed Mitigation tab for Risk 1001**.



Conducting a PCI DSS Compliance Review (3e)
vWorkstation
2024-09-04 11:05:59
Bradley Adams

SimpleRisk: Enterprise Risk Man
Not secure
https://172.30.0.5/management/management_review.php
Set Chrome as your default
Google Chrome isn't your default browser
Set as default
1 Submit Risk
2 Plan Mitigation
3 Perform Reviews
4 Plan Projects
5 Review Regularly
Actions
View Risk Scoring Details
Show Risk Score Over Time
Details
Mitigation
Review
Edit Mitigation
Accept Mitigation
9:05 AM
9/4/2024

Inherent Risk 7 High

Residual Risk 1.4 Low

ID #: 1001 Status: New

Subject : We do not ensure removal of test data and accounts from system components before the system becomes active / goes into production. (6.4.4)

Mitigation Submission Date: 09/04/2024

Planned Mitigation Date: 09/04/2024

Planning Strategy: Mitigate

Mitigation Effort: Minor

Mitigation Cost: $0 to $100,000

Mitigation Owner: Rick RiskOwner

Mitigation Team: IT Systems Management

Mitigation Percent: 80%

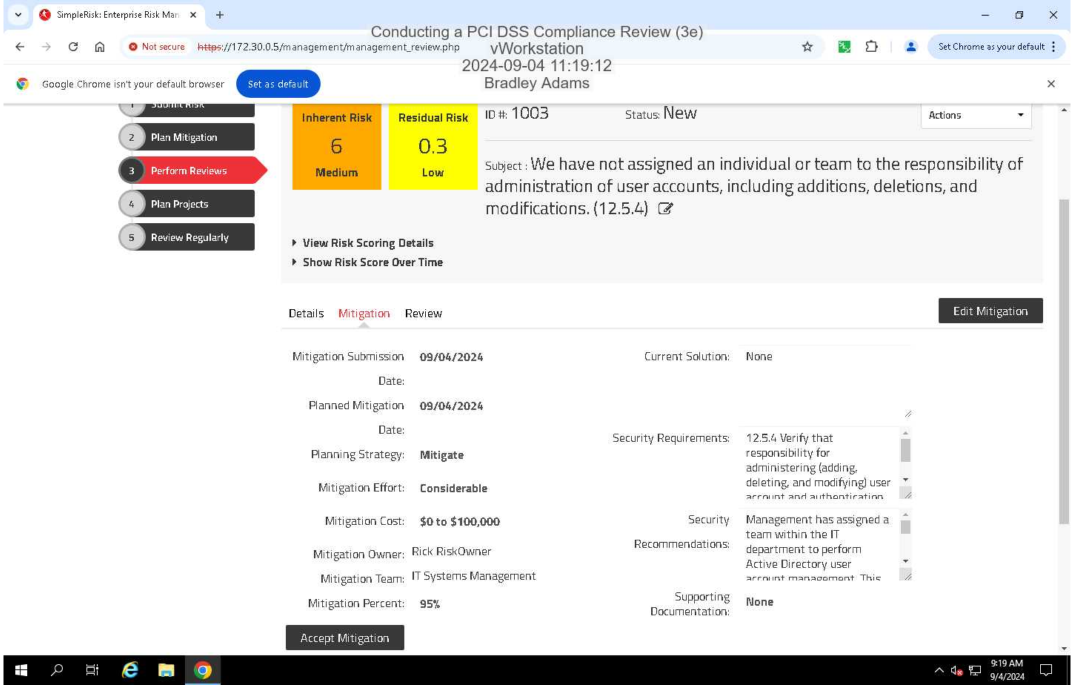
Current Solution: None

Security Requirements: 6.4.4 Verify that test data and accounts are removed before production systems become active

Security Recommendations: been assigned to review Active Directory test accounts and test data prior to any system becoming active into production. This

Supporting Documentation: None

**Make a screen capture** showing the **completed Mitigation tab for Risk 1003**.



Conducting a PCI DSS Compliance Review (3e)
vWorkstation
2024-09-04 11:19:12
Bradley Adams

SimpleRisk: Enterprise Risk Man
Not secure
https://172.30.0.5/management/management_review.php
Set Chrome as your default
Google Chrome isn't your default browser
Set as default
2 Plan Mitigation
3 Perform Reviews
4 Plan Projects
5 Review Regularly
Actions
View Risk Scoring Details
Show Risk Score Over Time
Details
Mitigation
Review
Edit Mitigation
Accept Mitigation
9:19 AM
9/4/2024

Inherent Risk 6 Medium

Residual Risk 0.3 Low

ID #: 1003 Status: New

Subject : We have not assigned an individual or team to the responsibility of administration of user accounts, including additions, deletions, and modifications. (12.5.4)

Mitigation Submission Date: 09/04/2024

Planned Mitigation Date: 09/04/2024

Planning Strategy: Mitigate

Mitigation Effort: Considerable

Mitigation Cost: $0 to $100,000

Mitigation Owner: Rick RiskOwner

Mitigation Team: IT Systems Management

Mitigation Percent: 95%

Current Solution: None

Security Requirements: 12.5.4 Verify that responsibility for administering (adding, deleting, and modifying) user account and authentication

Security Recommendations: Management has assigned a team within the IT department to perform Active Directory user account management. This

Supporting Documentation: None

**Provide examples** of your recommended mitigation actions.

**For 1001**: Members of the IT systems management team have been assigned to review Active Directory test accounts and test data prior to any system becoming active into production. This Mitigation does not address the root cause of the risk but does address the immediate risk, therefore the Mitigation Percent is 80. **For 1003**: Management has assigned a team within the IT department to perform Active Directory user account management. This includes policy creating a line of communication with HR for notifications of personnel changes. This does address the root cause of the risk, so the Mitigation Percent score is set to 95.