Conducting a PCI DSS Compliance Review (3e)

Managing Risk in Information Systems, Third Edition - Lab 02

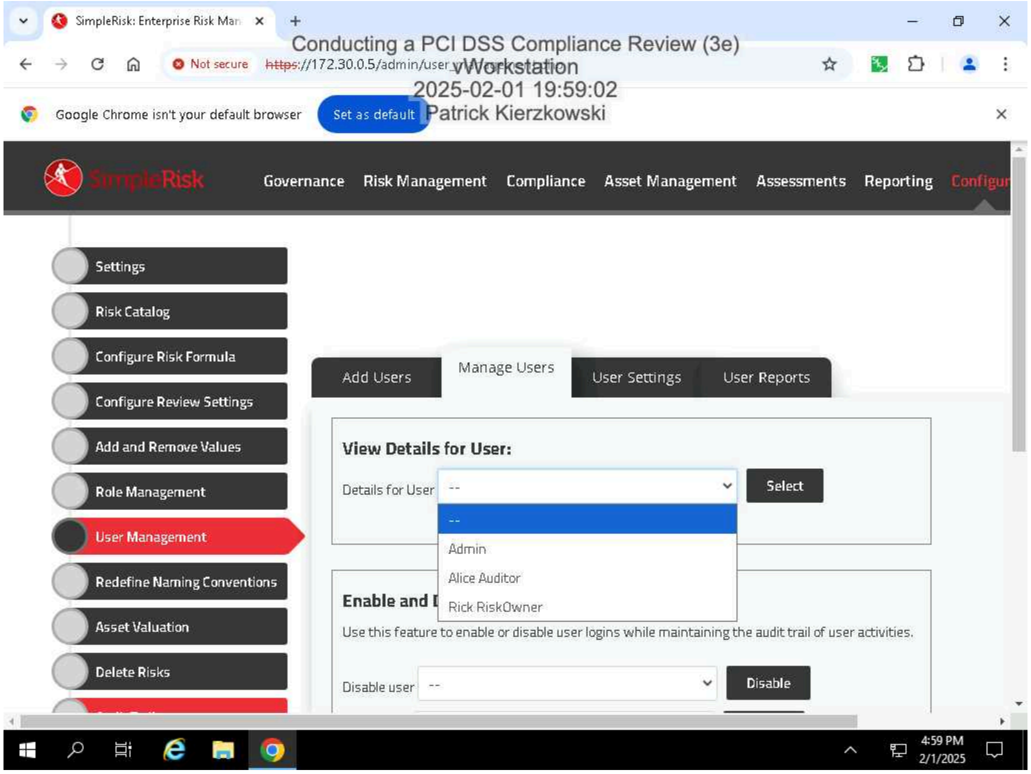
Student: Patrick Kierzkowski	Email: pxk405@francis.edu
Time on Task: 9 hours, 33 minutes	Progress: 100%

Report Generated: Monday, July 7, 2025 at 9:38 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
2025-02-01 19:59:02
Patrick Kierzkowski

https://172.30.0.5/admin/user_management.php

View Details for User:

Details for User: --

- --
- Admin
- Alice Auditor
- Rick RiskOwner

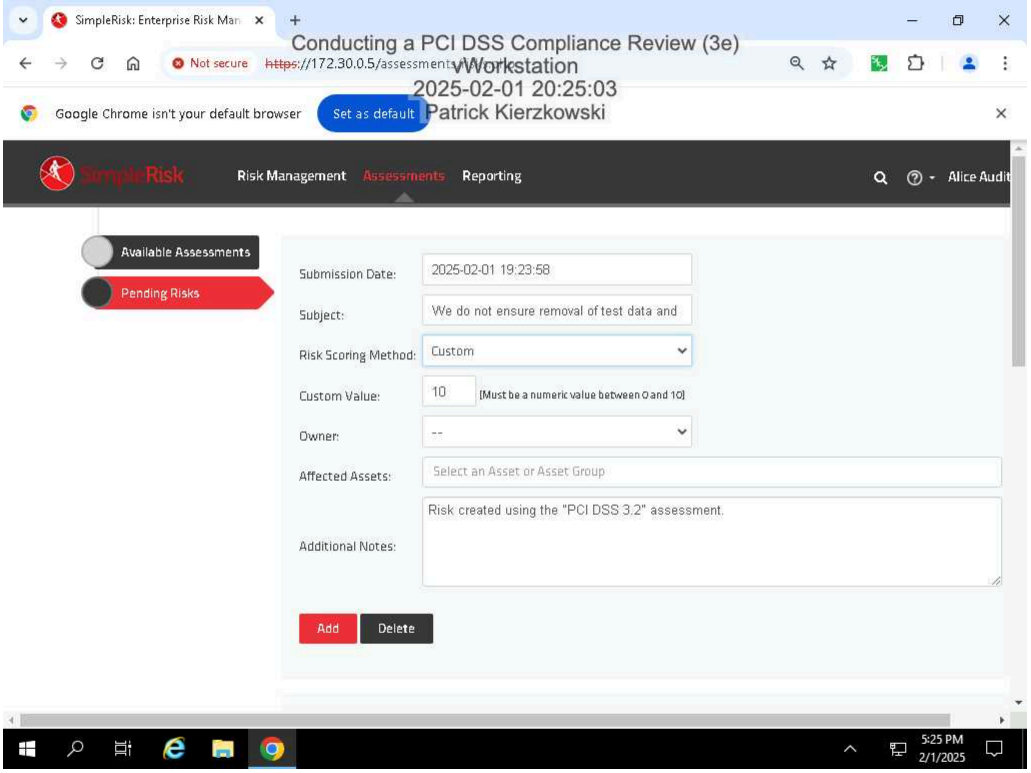
Enable and Disable

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

Disable user: --

Part 2: Identify Instances of Noncompliance

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



Submission Date: 2025-02-01 19:23:58

Subject: We do not ensure removal of test data and

Risk Scoring Method: Custom

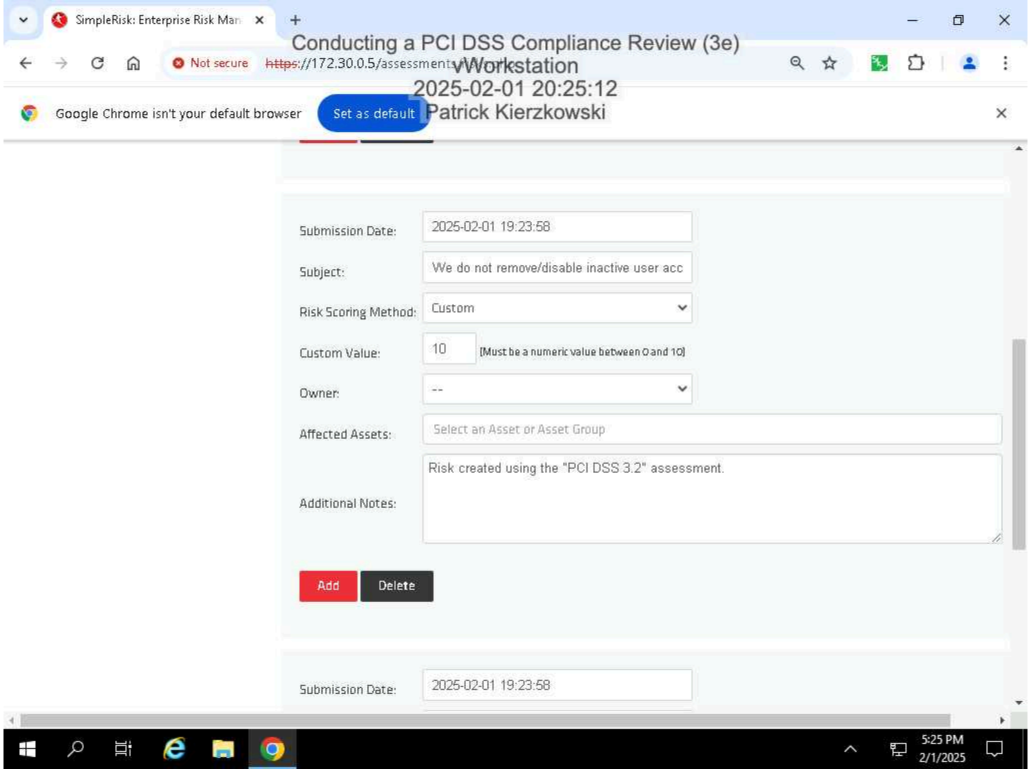
Custom Value: 10 [Must be a numeric value between 0 and 10]

Owner: --

Affected Assets: Select an Asset or Asset Group

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

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
Google Chrome isn't your default browser
Set as default
5:25 PM
2/1/2025

Conducting a PCI DSS Compliance Review (3e)
vWorkstation
2025-02-01 20:25:12
Patrick Kierzkowski

Submission Date: 2025-02-01 19:23:58

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: --

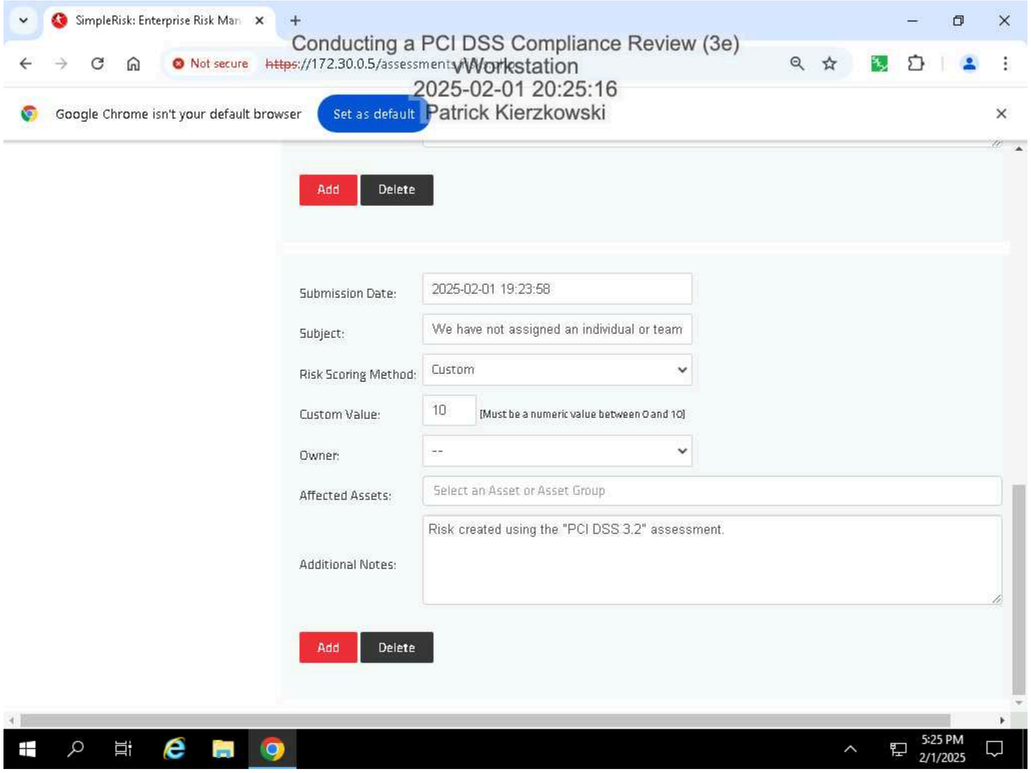
Affected Assets: Select an Asset or Asset Group

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

Add Delete

Submission Date: 2025-02-01 19:23:58

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
Google Chrome isn't your default browser
Set as default
5:25 PM
2/1/2025

Conducting a PCI DSS Compliance Review (3e)
vWorkstation
2025-02-01 20:25:16
Patrick Kierzkowski

Add Delete

Submission Date: 2025-02-01 19:23:58

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]

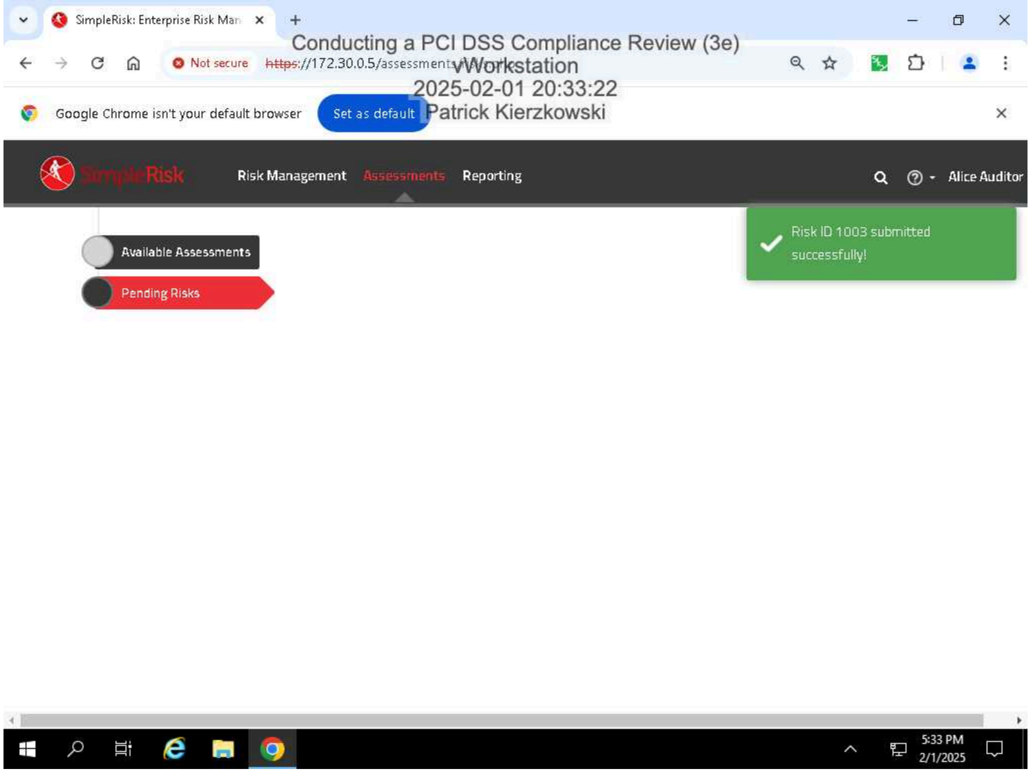
Owner: --

Affected Assets: Select an Asset or Asset Group

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

Add Delete

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

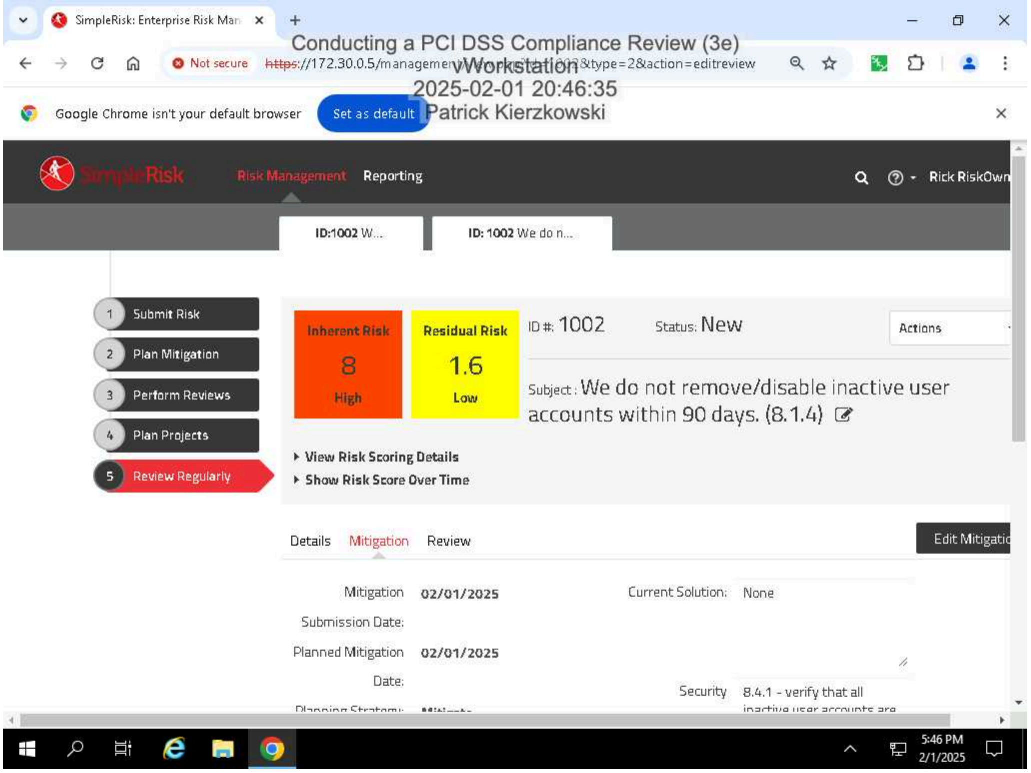


Conducting a PCI DSS Compliance Review (3e)
vWorkstation
2025-02-01 20:33:22
Patrick Kierzkowski

Risk ID 1003 submitted successfully!

Part 3: Review Risks and Set Mitigation Actions

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



Conducting a PCI DSS Compliance Review (3e)
vWorkstation
2025-02-01 20:46:35
Patrick Kierzkowski

https://172.30.0.5/management/view.php?id=1002&type=2&action=editreview

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: 02/01/2025

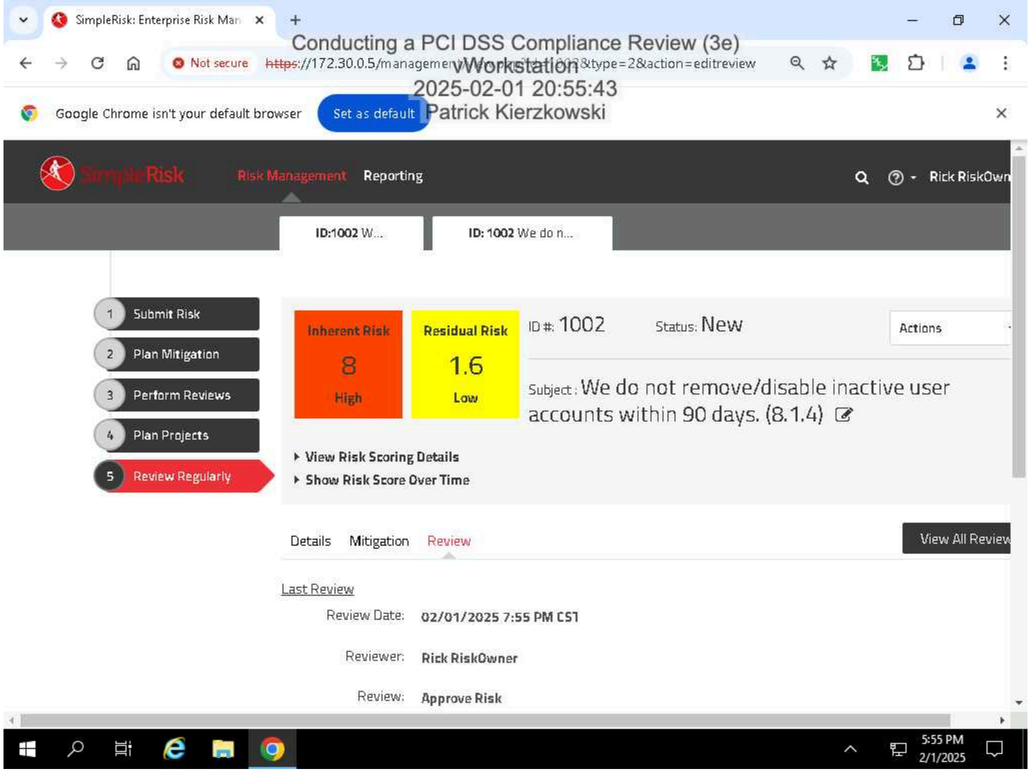
Planned Mitigation Date: 02/01/2025

Planning Strategy: Mitigate

Current Solution: None

Security: 8.4.1 - verify that all inactive user accounts are

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



Conducting a PCI DSS Compliance Review (3e)
vWorkstation
2025-02-01 20:55:43
Patrick Kierzkowski

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

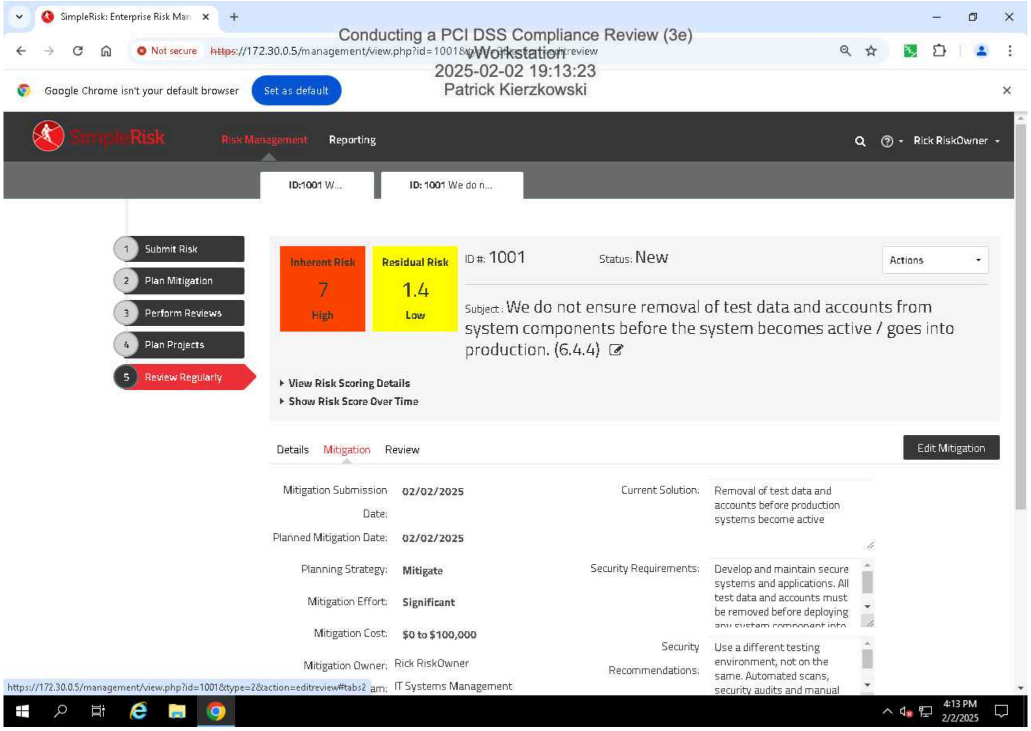
Review Date: 02/01/2025 7:55 PM CST

Reviewer: Rick RiskOwner

Review: Approve Risk

Challenge Exercise

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


SimpleRisk: Enterprise Risk Man
Not secure
~~https~~://172.30.0.5/management/view.php?id=1001&type=2&action=editreview
Google Chrome isn't your default browser
Set as default
SimpleRisk
Risk Management
Reporting
Rick RiskOwner
ID:1001 W...
ID: 1001 We do n...
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
https://172.30.0.5/management/view.php?id=1001&type=2&action=editreview#tabs2
4:13 PM
2/2/2025

Conducting a PCI DSS Compliance Review (3e)
vWorkstation
2025-02-02 19:13:23
Patrick Kierzkowski

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: 02/02/2025

Planned Mitigation Date: 02/02/2025

Planning Strategy: Mitigate

Mitigation Effort: Significant

Mitigation Cost: $0 to $100,000

Mitigation Owner: Rick RiskOwner

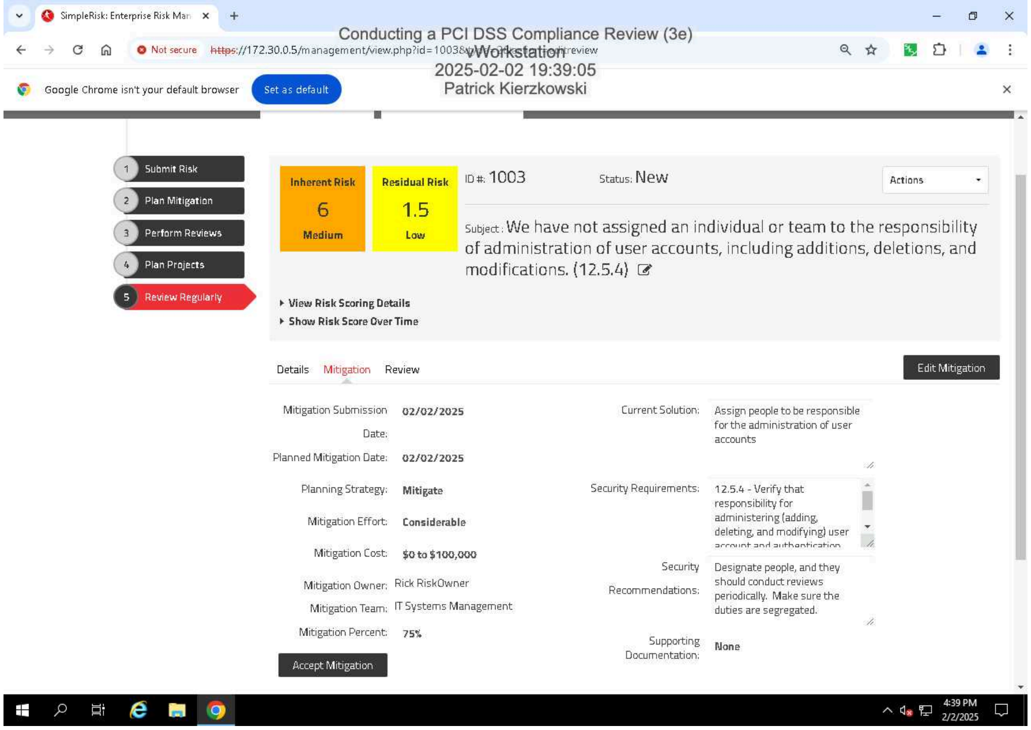
am: IT Systems Management

Current Solution: Removal of test data and accounts before production systems become active

Security Requirements: Develop and maintain secure systems and applications. All test data and accounts must be removed before deploying any system component into

Security Recommendations: Use a different testing environment, not on the same. Automated scans, security audits and manual

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


SimpleRisk: Enterprise Risk Man
Not secure
https://172.30.0.5/management/view.php?id=1003&type=2&active=review
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
4:39 PM
2/2/2025

Conducting a PCI DSS Compliance Review (3e)
vWorkstation
2025-02-02 19:39:05
Patrick Kierzkowski

Inherent Risk: 6 Medium

Residual Risk: 1.5 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: 02/02/2025

Planned Mitigation Date: 02/02/2025

Planning Strategy: Mitigate

Mitigation Effort: Considerable

Mitigation Cost: $0 to $100,000

Mitigation Owner: Rick RiskOwner

Mitigation Team: IT Systems Management

Mitigation Percent: 75%

Current Solution: Assign people to be responsible for the administration of user accounts

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

Security Recommendations: Designate people, and they should conduct reviews periodically. Make sure the duties are segregated.

Supporting Documentation: None

Provide examples of your recommended mitigation actions.

For 6.4.4, using a different environment for testing is beneficial as it can prevent security vulnerabilities and make sure its isolated. Automated scans can check the isolated enviornemt to ensure there are no vulnerabilities. The security audit will ensure that proper controls and isolation are in place.
For 12.5.4 a team or a few individuals should be assigned to the responsibility of administration of user accounts, where checks should be made often. People apart of the team should have their duties split, so no one has full power.