

Conducting a PCI DSS Compliance Review (3e)

Managing Risk in Information Systems, Third Edition - Lab 02

Student:

Bradley Adams

Email:

badams10@my.athens.edu

Time on Task:

1 hour, 27 minutes

Progress:

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.

The screenshot shows the SimpleRisk User Management interface. On the left, a sidebar menu lists various administrative functions: Settings, Risk Catalog, Configure Risk Formula, Configure Review Settings, Add and Remove Values, Role Management, **User Management** (which is highlighted with a red arrow), Redefine Naming Conventions, Asset Valuation, Delete Risks, Audit Trail, Extras, Announcements, Register & Upgrade, and Health Check. The main content area has tabs for Add Users, Manage Users (which is selected and highlighted with a black border), User Settings, and User Reports. Under the Manage Users tab, there's a section titled 'View Details for User:' with a dropdown menu showing three users: Admin, Alice Auditor, and Rick RiskOwner. Below this is a section titled 'Enable and Disable User' with dropdown menus for 'Disable user' and 'Enable user'. Further down are sections for 'Delete an Existing User' (with a 'Delete' button) and 'Password Reset'. The top navigation bar includes links for Governance, Risk Management, Compliance, Asset Management, Assessments, Reporting, and Configure, along with a search bar and user profile information for Bradley Adams.

Part 2: Identify Instances of Noncompliance

Conducting a PCI DSS Compliance Review (3e)

Managing Risk in Information Systems, Third Edition - Lab 02

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

The screenshot shows the SimpleRisk Enterprise Risk Management software interface. The title bar indicates "Conducting a PCI DSS Compliance Review (3e)" and the date "2024-09-04 10:25:20". The user is Bradley Adams, and the session is Alice Auditor. The navigation menu includes Risk Management, Assessments (which is selected), and Reporting. On the left, there are two buttons: "Available Assessments" (grey) and "Pending Risks" (red). The main area displays a single risk entry:

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

At the bottom of the form are "Add" and "Delete" buttons. The status bar at the bottom right shows "8:35 AM 9/4/2024".

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

The screenshot shows the SimpleRisk Enterprise Risk Management software interface, identical to the previous one but with two risk entries listed. The title bar, user information, and navigation menu are the same. The "Pending Risks" button is highlighted.

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

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

At the bottom of the form are "Add" and "Delete" buttons. The status bar at the bottom right shows "8:35 AM 9/4/2024".

Conducting a PCI DSS Compliance Review (3e)

Managing Risk in Information Systems, Third Edition - Lab 02

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

The screenshot shows a web browser window for 'SimpleRisk: Enterprise Risk Man...' at the URL 'https://172.30.0.5/assessments/risks.php'. The title bar indicates 'Conducting a PCI DSS Compliance Review (3e)' and the date '2024-09-04 10:25:39'. The main content area displays two risk entries. Each entry includes fields for Owner (set to 'Bradley Adams'), Affected Assets (a dropdown menu), Additional Notes (a text area), and two buttons: 'Add' and 'Delete'. The first risk entry has a Submission Date of '2024-09-04 10:24:56', Subject 'We have not assigned an individual or team', Risk Scoring Method 'Custom', and a Custom Value of '10'. The second risk entry has a Submission Date of '2024-09-04 10:34:58', Subject 'We have not assigned an individual or team', Risk Scoring Method 'Custom', and a Custom Value of '10'. The bottom status bar shows the date '9/4/2024' and time '8:25 AM'.

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

The screenshot shows a web browser window for 'SimpleRisk: Enterprise Risk Man...' at the URL 'https://172.30.0.5/assessments/risks.php'. The title bar indicates 'Conducting a PCI DSS Compliance Review (3e)' and the date '2024-09-04 10:34:58'. The top navigation bar includes the SimpleRisk logo, 'Risk Management', 'Assessments', 'Reporting', a search icon, and a user dropdown for 'Alice Auditor'. Below the navigation is a horizontal menu with two items: 'Available Assessments' (grey button) and 'Pending Risks' (red button with a white arrow). The main content area is empty, showing only the header for the pending risks section. The bottom status bar shows the date '9/4/2024' and time '8:34 AM'.

Part 3: Review Risks and Set Mitigation Actions

Conducting a PCI DSS Compliance Review (3e)

Managing Risk in Information Systems, Third Edition - Lab 02

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

Inherent Risk: 8
Residual Risk: 1.6
Status: New
Subject: We do not remove/disable inactive user accounts within 90 days.
(8.1.4)

Mitigation Submission: 09/04/2024
Current Solution: None
Planned Mitigation: 09/04/2024
Date:
Planning Strategy: Mitigate
Security Requirements: B.4.1 - Verify that all inactive user accounts are disabled
Mitigation Effort: Minor
Mitigation Cost: \$0 to \$100,000
Mitigation Owner: Rick RiskOwner
Mitigation Team: IT Systems Management
Mitigation Percent: 80%
Security Recommendations: Members of the IT department have already been assigned to perform an ad-hoc review of Active Directory to identify and
Supporting Documentation: None
Accept Mitigation

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

Inherent Risk: 8
Residual Risk: 1.6
Status: New
Subject: We do not remove/disable inactive user accounts within 90 days.
(8.1.4)

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.

The screenshot shows the 'Mitigation' tab for Risk 1001. The risk details are as follows:

| Inherent Risk | Residual Risk |
|---------------|---------------|
| 7 High | 1.4 Low |

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: 09/04/2024
Planned Mitigation: 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
Recommendations: been assigned to review Active Directory test accounts and test data prior to any system becoming active into production. This
Supporting Documentation: None

Action Buttons: Accept Mitigation, Edit Mitigation

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

The screenshot shows the 'Mitigation' tab for Risk 1003. The risk details are as follows:

| Inherent Risk | Residual Risk |
|---------------|---------------|
| 6 Medium | 0.3 Low |

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: 09/04/2024
Planned Mitigation: 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
Recommendations: Management has assigned a team within the IT department to perform Active Directory user account management. This
Supporting Documentation: None

Action Buttons: Accept Mitigation, Edit Mitigation

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.