

# 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.

The screenshot shows the SimpleRisk software interface. The top navigation bar includes links for Governance, Risk Management, Compliance, Asset Management, Assessments, Reporting, and Configuration. On the left, a sidebar lists various management functions: Settings, Risk Catalog, Configure Risk Formula, Configure Review Settings, Add and Remove Values, Role Management, User Management (which is highlighted in red), Redefine Naming Conventions, Asset Valuation, and Delete Risks. The main content area is titled 'View Details for User:' and contains a dropdown menu for 'Details for User' with options: Admin, Alice Auditor, and Rick RiskOwner. Below this is a section titled 'Enable and Disable User' with a dropdown menu for 'Disable user' containing the same three names. A note states: 'Use this feature to enable or disable user logins while maintaining the audit trail of user activities.' The bottom status bar shows the date and time as 2/1/2025 and 4:59 PM.

### 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 a web browser window for 'SimpleRisk: Enterprise Risk Management' at the URL <https://172.30.0.5/assessments>. The title bar indicates the page is titled 'Conducting a PCI DSS Compliance Review (3e)' and was last modified on '2025-02-01 20:25:03' by 'Patrick Kierzkowski'. The browser status bar says 'Google Chrome isn't your default browser' and has a 'Set as default' link.

The main interface shows a navigation bar with 'Risk Management', 'Assessments' (highlighted in red), and 'Reporting'. Below the navigation is a toolbar with 'Available Assessments' and 'Pending Risks' buttons. The 'Pending Risks' button is highlighted with a red arrow pointing to it.

The central area displays a risk entry form:

- 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.

At the bottom of the form are 'Add' and 'Delete' buttons.

The taskbar at the bottom of the screen shows standard Windows icons for Start, Search, Task View, Internet Explorer, File Explorer, and Google Chrome. The system tray shows the date and time as 2/1/2025 5:25 PM.

# Conducting a PCI DSS Compliance Review (3e)

## Managing Risk in Information Systems, Third Edition - Lab 02

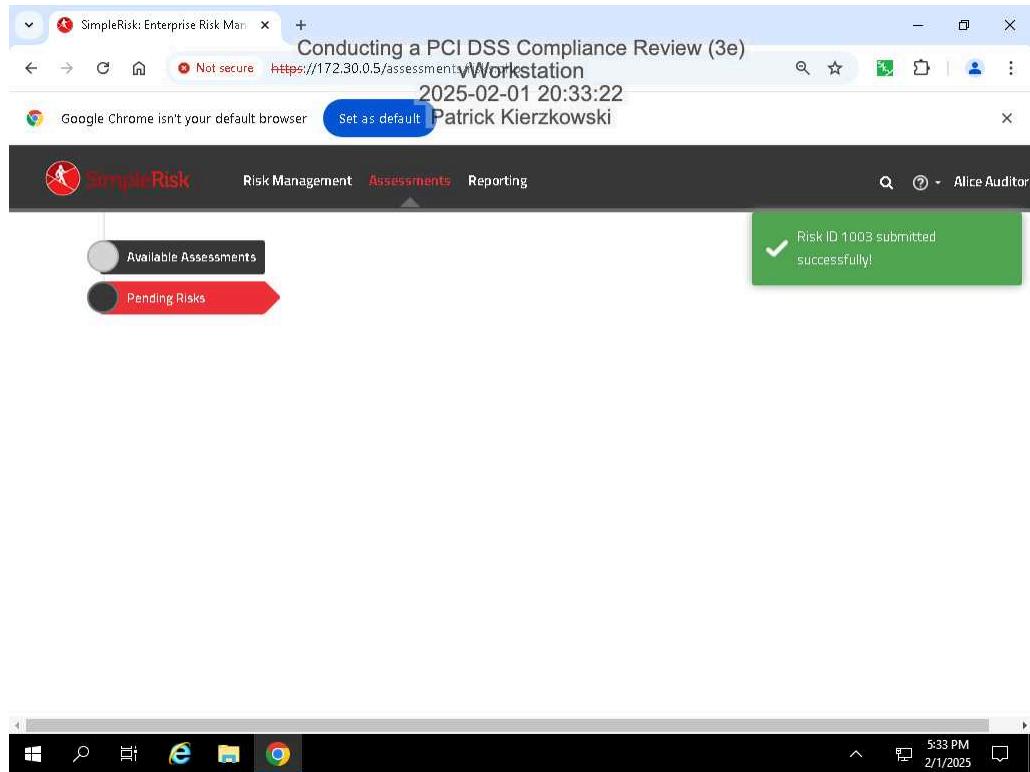
### 12. Make a screen capture showing the second risk entry on the Pending Risks page.

The screenshot shows a web browser window titled "Conducting a PCI DSS Compliance Review (3e)" with the URL <https://172.30.0.5/assessment>. The page displays a risk entry form. The submission date is 2025-02-01 20:25:12. The subject is "We do not remove/disable inactive user acc". The risk scoring method is set to "Custom". The custom value is 10. The owner is listed as "--". The affected assets field is empty, showing "Select an Asset or Asset Group". The additional notes field contains the text "Risk created using the \"PCI DSS 3.2\" assessment.". At the bottom, there are "Add" and "Delete" buttons. The browser status bar at the bottom right shows the date and time as 2/1/2025 5:25 PM.

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

The screenshot shows a web browser window titled "Conducting a PCI DSS Compliance Review (3e)" with the URL <https://172.30.0.5/assessment>. The page displays a risk entry form. The submission date is 2025-02-01 20:25:16. The subject is "We have not assigned an individual or team". The risk scoring method is set to "Custom". The custom value is 10. The owner is listed as "--". The affected assets field is empty, showing "Select an Asset or Asset Group". The additional notes field contains the text "Risk created using the \"PCI DSS 3.2\" assessment.". At the bottom, there are "Add" and "Delete" buttons. The browser status bar at the bottom right shows the date and time as 2/1/2025 5:25 PM.

**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.

The screenshot shows a web browser window titled "Conducting a PCI DSS Compliance Review (3e)" with the URL <https://172.30.0.5/management/reviews?&type=2&action=editreview>. The page displays a risk review for a user account. The main interface includes a navigation bar with "Simple Risk", "Risk Management", and "Reporting". On the left, there's a sidebar with five steps: "Submit Risk", "Plan Mitigation", "Perform Reviews", "Plan Projects", and "Review Regularly". The main content area shows a risk card for "ID: 1002 Workstation" with the subject "We do not remove/disable inactive user accounts within 90 days. (8.1.4)". The risk score is 8 (High) for Inherent Risk and 1.6 (Low) for Residual Risk. The status is "New". Below the card, there are links to "View Risk Scoring Details" and "Show Risk Score Over Time". At the bottom, tabs for "Details", "Mitigation", and "Review" are visible, along with an "Edit Mitigation" button. The Windows taskbar at the bottom shows the date as 2/1/2025 and the time as 5:46 PM.

# Conducting a PCI DSS Compliance Review (3e)

Managing Risk in Information Systems, Third Edition - Lab 02

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

The screenshot shows a web browser window for 'SimpleRisk: Enterprise Risk Management' at the URL <https://172.30.0.5/management?&type=2&action=editreview>. The title bar says 'Conducting a PCI DSS Compliance Review (3e)'. The top navigation bar includes 'Risk Management' and 'Reporting'. The main content area displays Risk ID 1002, which has been reviewed by 'Patrick Kierzkowski' on '2025-02-01 20:55:43'. The risk details show an Inherent Risk score of 8 (High) and a Residual Risk score of 1.6 (Low). The status is 'New' and the subject is 'We do not remove/disable inactive user accounts within 90 days. (8.1.4)'. Below the risk details, there are links to 'View Risk Scoring Details' and 'Show Risk Score Over Time'. A navigation bar at the bottom includes 'Details', 'Mitigation', 'Review' (which is highlighted in red), and 'View All Review'. The taskbar at the bottom of the screen shows various icons and the date/time as 5:55 PM 2/1/2025.

## Challenge Exercise

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

The screenshot shows a web browser window for SimpleRisk Enterprise Risk Management. The title bar reads "Conducting a PCI DSS Compliance Review (3e)" and "Workstation". The address bar shows the URL "https://172.30.0.5/management/view.php?id=1001&type=2&action=edit&review#tab2". The user is Patrick Kierzkowski. The main interface displays Risk 1001 with the 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)". The risk score is 7 (High) for Inherent Risk and 1.4 (Low) for Residual Risk. The status is New. The mitigation tab is selected, showing details like Mitigation Submission (02/02/2025), Current Solution (Removal of test data and accounts before production systems become active), and Security Requirements (Develop and maintain secure systems and applications. All test data and accounts must be removed before deploying any system component into production). The review tab is also visible at the bottom.

# Conducting a PCI DSS Compliance Review (3e)

Managing Risk in Information Systems, Third Edition - Lab 02

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

The screenshot shows a web browser window titled "Conducting a PCI DSS Compliance Review (3e)" with the URL <https://172.30.0.5/management/view.php?id=1003&view=Mitigation>. The page displays a risk card for Risk ID #1003, which has an Inherent Risk score of 6 (Medium) and a Residual Risk score of 1.5 (Low). The status is New. A subject note states: "We have not assigned an individual or team to the responsibility of administration of user accounts, including additions, deletions, and modifications. (12.5.4)". Below the card, there are five navigation buttons: Submit Risk, Plan Mitigation, Perform Reviews, Plan Projects, and Review Regularly. The "Review Regularly" button is highlighted in red. The main content area is divided into Details, Mitigation, and Review tabs, with the Mitigation tab selected. Under the Mitigation tab, the following details are listed:

Mitigation Submission Date:	02/02/2025	Current Solution:	Assign people to be responsible for the administration of user accounts
Planned Mitigation Date:	02/02/2025	Planning Strategy:	Mitigate
Mitigation Effort:	Considerable	Security Requirements:	12.5.4 - Verify that responsibility for administering (adding, deleting, and modifying) user account and authentication
Mitigation Cost:	\$0 to \$100,000	Security Recommendations:	Designate people, and they should conduct reviews periodically. Make sure the duties are segregated.
Mitigation Owner:	Rick RiskOwner	Supporting Documentation:	None
Mitigation Team:	IT Systems Management		
Mitigation Percent:	75%		

At the bottom left is a "Accept Mitigation" button, and at the bottom right is an "Edit Mitigation" button. The browser status bar shows the date as 2/2/2025 and the time as 4:39 PM.

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 environment 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.