

# Developing a Risk Mitigation Plan (3e)

Managing Risk in Information Systems, Third Edition - Lab 07

Student:

Bradley Adams

Email:

badams10@my.athens.edu

Time on Task:

1 hour, 27 minutes

Progress:

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.

The screenshot shows a web-based application titled "SimpleRisk Enterprise Risk Management". The main navigation bar includes links for Governance, Risk Management (which is currently selected), Compliance, Bradly Adams (user profile), Assessments, Reporting, Configure, and Admin. The title bar also displays the URL "172.30.0.5/management/plan\_mitigations.php" and the page title "Developing a Risk Mitigation Plan (3e) vWorkstation".

The main content area is titled "Risk List" and shows a single risk entry with ID # 1001. The risk details are as follows:

- Inherent Risk:** 0.4 (Low)
- Residual Risk:** 0.4 (Low)
- Status:** New
- Subject:** Unauthorized access to computers after cracking uncomplex passwords

A sidebar on the left lists five steps: 1. Submit Risk, 2. Plan Mitigation (highlighted in red), 3. Perform Reviews, 4. Plan Projects, and 5. Review Regularly.

Below the risk details, there is a section for "Classic Risk Scoring" with fields for Likelihood (Remote) and Impact (Insignificant). A formula calculates the risk score:  $RISK = (Likelihood \times Impact) \times (10 / 25) = 0.4$ .

At the bottom of the page, there are tabs for Details, Mitigation, Review, and Edit Details. The Mitigation tab is active. The status bar at the bottom right shows the date and time as 10:09 AM 11/8/2024.

# Developing a Risk Mitigation Plan (3e)

Managing Risk in Information Systems, Third Edition - Lab 07

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

The screenshot shows the 'Developing a Risk Mitigation Plan (3e)' page. At the top, there is a navigation bar with links for 'Submit Risk', 'Plan Mitigation' (which is highlighted in red), 'Perform Reviews', 'Plan Projects', and 'Review Regularly'. Below this is a summary card with 'Inherent Risk' (6, Medium) and 'Residual Risk' (0.3, Low). The main content area displays mitigation details: Submission Date (11/08/2024), Current Solution (None), Planned Mitigation Date (11/22/2024), Security Requirements (PCI DSS compliance requirements), Planning Strategy (Mitigate), Mitigation Effort (Considerable), Mitigation Cost (\$0 to \$100,000), Recommendations (Update information security policy section 2.2 and change the domain-wide password policy accordingly), Mitigation Owner (Admin), Mitigation Team (Information Security, Windows), Mitigation Percent (95%), Supporting Documentation (None), and an 'Accept Mitigation' button. The status is listed as 'New'.

## Part 2: Conduct a Management Review

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

The screenshot shows the 'Developing a Risk Mitigation Plan (3e)' page with a status of 'Mitigation Planned'. The 'Review' tab is selected. The review date is set to 11/08/2024, the reviewer is Admin, and the review status is 'Approve Risk'. The next step is 'Consider for Project'. A project name is listed as 'Information security policy and domain policy update'. A comment field contains the text 'Update the domain policy after the information security policy changes have been approved.' There is also a note about the next review date being 05/07/2025 and a question if a different date is desired. The status is now 'Mitigation Planned'.

# Developing a Risk Mitigation Plan (3e)

Managing Risk in Information Systems, Third Edition - Lab 07

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

The screenshot shows a web-based risk management application titled "SimpleRisk Enterprise Risk Man...". The main navigation bar includes links for Governance, Risk Management, Compliance, Bradley Adapte..., Assessments, Reporting, Configure, and Admin. The current page is "Risk Management". A sub-menu on the left lists five items: 1. Submit Risk, 2. Plan Mitigation, 3. Perform Reviews, 4. Plan Projects, and 5. Review Regularly. The main content area displays a risk record with the ID "ID: 1001 Unauthorized...". The risk has an Inherent Risk score of 6 (Medium) and a Residual Risk score of 0.3 (Low). The status is "Closed". The subject of the risk is "Unauthorized access to computers after cracking uncomplex passwords". Below the risk details are two buttons: "View Risk Scoring Details" and "Show Risk Score Over Time". At the bottom of the page are tabs for "Details", "Mitigation", and "Review", with "Edit Details" and "Affected Assets" buttons. The system status bar at the bottom right shows "10:23 AM" and "11/8/2024".

# Developing a Risk Mitigation Plan (3e)

Managing Risk in Information Systems, Third Edition - Lab 07

## 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.**

The screenshot shows the SimpleRisk software interface for managing risk mitigation plans. The main window title is "Developing a Risk Mitigation Plan (3e)" and the subject is "Leak of sensitive information stored in cleartext files". The risk score is displayed as Inherent Risk (8, High) and Residual Risk (0.4, Low). The navigation menu on the left includes "Submit Risk", "Plan Mitigation" (selected), "Perform Reviews", "Plan Projects", and "Review Regularly". The "Mitigation" tab is active, showing the following details:

Mitigation Submission	11/08/2024	Current Solution	There are no current solutions
Date:			
Planned Mitigation	11/22/2024		
Date:			
Planning Strategy:	Mitigate	Security Requirements:	Prevent the leak of sensitive information stored in cleartext files
Mitigation Effort:	Considerable		
Mitigation Cost:	\$0 to \$100,000	Security	Implementation of data classification and minimization controls, Encryption controls, and Access Control and Auditing
Mitigation Owner:	Admin	Recommendations:	
Mitigation Team:	Information Security, Network, Windows		
Mitigation Percent:	95%	Supporting Documentation:	None

At the bottom of the mitigation section is a "Accept Mitigation" button. The status bar at the bottom right shows the time as 11:23 AM and the date as 11/8/2024.