

# Developing a Risk Mitigation Plan (3e)

Managing Risk in Information Systems, Third Edition - Lab 07

Student:

Patrick Kierzkowski

Email:

pxk405@francis.edu

Time on Task:

5 hours, 0 minutes

Progress:

100%

Report Generated: Monday, July 7, 2025 at 9:41 PM

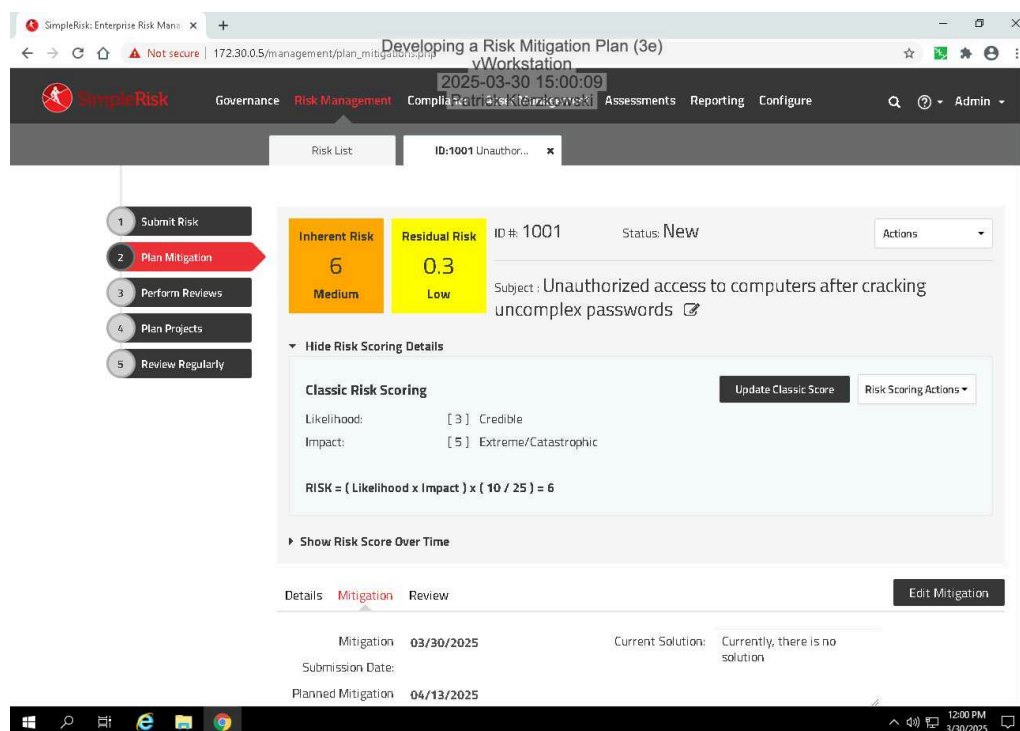
## Guided Exercises

### Part 1: Prepare a Risk Mitigation Plan

13. Make a screen capture showing the **updated inherent risk value**.

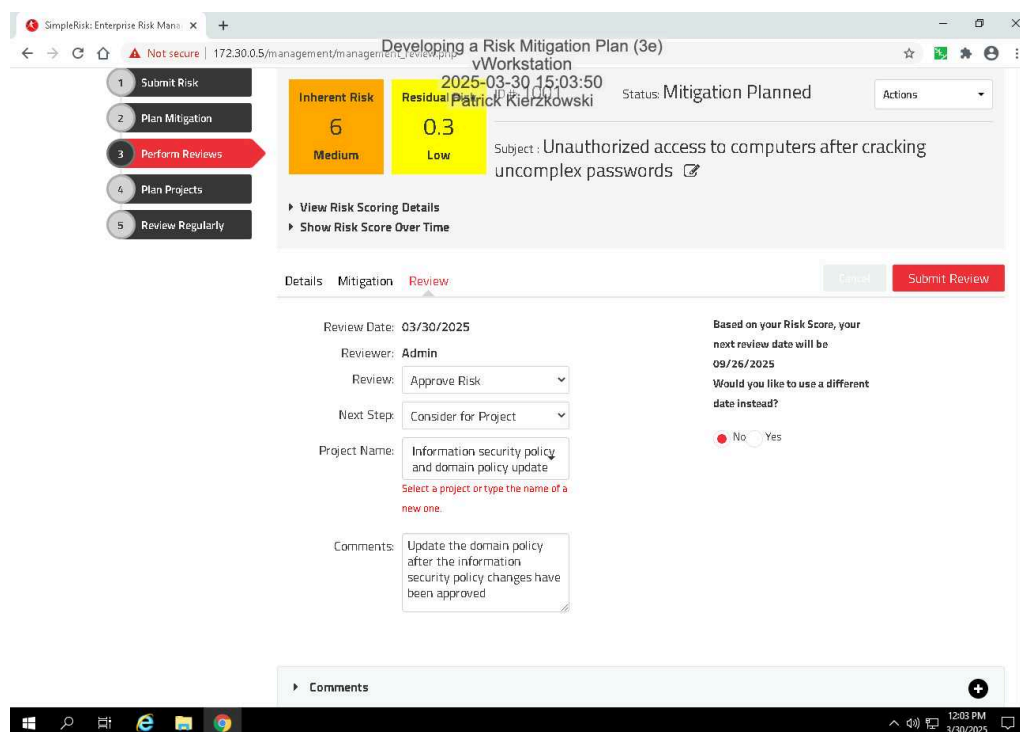
The screenshot displays the SimpleRisk Enterprise Risk Management web application. The interface includes a navigation menu on the left with options: Submit Risk, Plan Mitigation (highlighted), Perform Reviews, Plan Projects, and Review Regularly. The main content area shows the details for a risk with ID # 1001, Status: New. The risk is titled "Unauthorized access to computers after cracking uncomplex passwords". The Inherent Risk is 0.4 (Low) and the Residual Risk is 0.4 (Low). A green notification banner at the top right states "Risk scoring was updated successfully." Below the risk details, the "Classic Risk Scoring" section shows the calculation:  $RISK = (Likelihood \times Impact) \times (10 / 25) = 0.4$ . The submission date is 11/02/2020, and the risk source is Admin. The bottom of the screen shows the Windows taskbar with the time 11:55 AM on 3/30/2025.

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



## Part 2: Conduct a Management Review

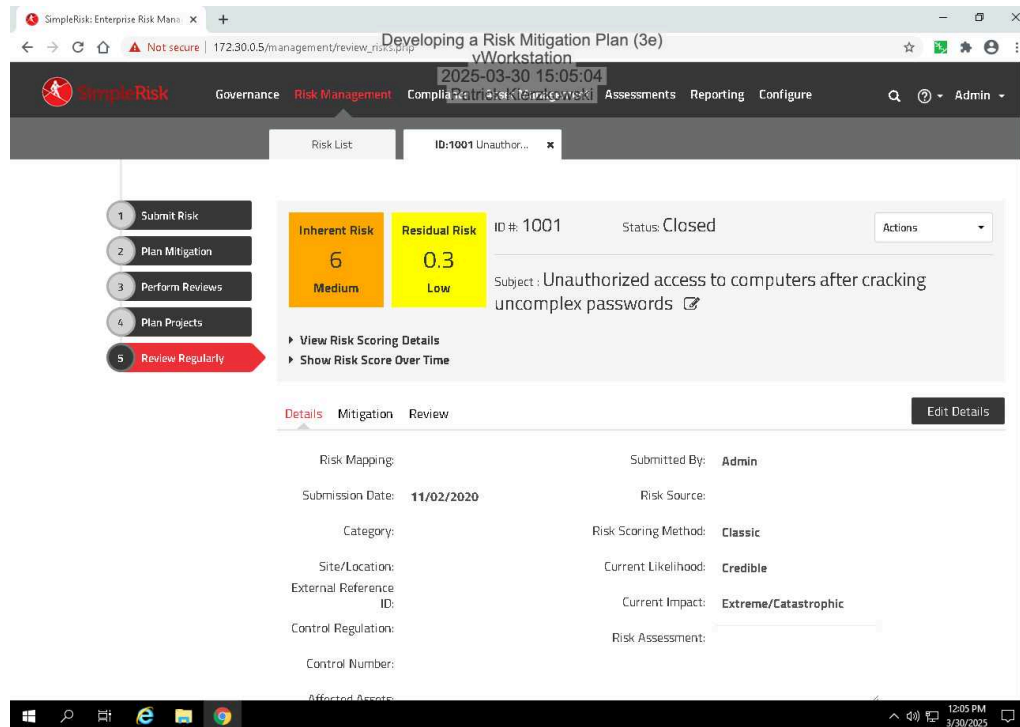
### 9. Make a screen capture showing the **completed Mitigation Review** page.



# Developing a Risk Mitigation Plan (3e)

## Managing Risk in Information Systems, Third Edition - Lab 07

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



### 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.

One security control that reduces asset value is to only collect and store the data that is needed. Extra data would mean that there is more information that could be stolen. Another security control that would reduce vulnerability severity is to regularly conduct patch updates. This would make it harder for hackers to exploit former vulnerabilities. Finally the security control that would reduce threat impact is to split the network into smaller sections. This means that if someone were to break in, they won't have access to everything.

**Make a screen capture** showing your **completed Risk Mitigation plan in SimpleRisk**.

